

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)
)
Takayuki HASEBE, et al.) Group Art Unit: To Be Assigned
)
Serial No.: To Be Assigned) Examiner: To Be Assigned
)
Filed: April 13, 2000) #3
) 7-11-00
) P.Z.
For: SIGNATURE CREATING APPARATUS,)
SIGNATURE VERIFICATION APPARATUS)
AND SIGNATURE APPARATUS)



**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. §1.55**

*Assistant Commissioner for Patents
Washington, D.C. 20231*

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, Applicants submit herewith a certified copy of the following foreign application:

Japanese Patent Application No. 11-151709 filed May 31, 1999.

It is respectfully requested that Applicants be given the benefit of the foreign filing date, as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY, LLP

Dated: April 13, 2000

By: _____

James D. Halsey, Jr.
Registration No. 22,729

700 Eleventh Street, N.W., Suite 500
Washington, D.C. 20001
(202) 434-1500

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENTjc688 U.S. PTO
09/549551
04/14/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
in this Office.

出 願 年 月 日
Date of Application:

1999年 5月31日

願 番 号
Application Number:

平成11年特許願第151709号

願 人
Applicant(s):

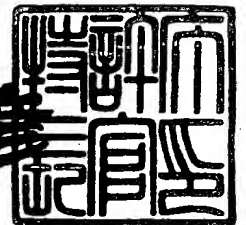
富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 2月18日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-300732

【書類名】 特許願

【整理番号】 9950661

【提出日】 平成11年 5月31日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00
H04L 9/32

【発明の名称】 署名作成装置および署名検証装置ならびに署名装置

【請求項の数】 16

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 長谷部 高行

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 小谷 誠剛

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 秋山 良太

【発明者】

 【住所又は居所】 東京都港区芝浦四丁目15番33号 株式会社富士通ビー・エス・シー内

 【氏名】 佐々木 孝興

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100089118

【弁理士】

【氏名又は名称】 酒井 宏明

【手数料の表示】

【予納台帳番号】 036711

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9717671

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 署名作成装置および署名検証装置ならびに署名装置

【特許請求の範囲】

【請求項 1】 デジタル署名を作成する署名作成装置において、時刻認証機関によってのみ時刻情報が設定される時計と、前記時刻情報および作成装置を特定するための装置 ID を平文に連結する連結手段と、

前記連結手段により作成された連結データ、および署名作成専用の鍵を用いて前記デジタル署名を作成する署名作成手段と、を備えることを特徴とする署名作成装置。

【請求項 2】 前記連結手段は、前記時刻情報および前記装置 ID に加えて、デジタル署名を作成した者を特定するための個人特定情報を前記平文に連結することを特徴とする請求項 1 に記載の署名作成装置。

【請求項 3】 前記個人特定情報を記憶する記憶手段と、前記記憶手段の記憶内容の更新を行う更新者が、正当な権限を有する者であるか否かを判断する判断手段と、

前記判断手段により前記更新者が正当な権限を有する者であると判断された場合にのみ、前記記憶手段の記憶内容を更新する更新手段とを備えることを特徴とする請求項 2 に記載の署名作成装置。

【請求項 4】 前記装置 ID は、書き換え不可能な記憶手段に記憶されていることを特徴とする請求項 1～3 のいずれか一つに記載の署名作成装置。

【請求項 5】 前記時計の動作状態を確認する確認手段を備え、前記署名作成手段は、前記確認手段により前記時計が正常に動作していることが確認された場合にのみ、前記デジタル署名を作成することを特徴とする請求項 1～4 のいずれか一つに記載の署名作成装置。

【請求項 6】 前記署名作成手段は、前記確認手段により前記時計が正常に動作していないと確認された場合、前記署名作成専用の鍵の利用を停止し、前記時刻情報を含まない連結情報と前記署名作成専用の鍵以外の鍵とを用いて、デジタル署名を作成することを特徴とする請求項 5 に記載の署名作成装置。

【請求項 7】 前記確認手段は、前記時計の駆動電圧としきい値との比較結果に基づいて、前記時計の動作状態を確認することを特徴とする請求項 5 または 6 に記載の署名作成装置。

【請求項 8】 前記確認手段は、一時点前の前記時計の計時結果と、現時点の計時結果との比較結果に基づいて、前記時計の動作状態を確認することを特徴とする請求項 5 または 6 に記載の署名作成装置。

【請求項 9】 前記確認手段は、前記時計が正常動作している場合、フラグをオンにし、前記時計が正常動作していない場合、前記フラグをオフにし、

前記署名作成手段は、前記フラグがオンにされている場合にのみ、前記デジタル署名を作成することを特徴とする請求項 5 または 6 に記載の署名作成装置。

【請求項 1 0】 前記時刻認証機関に設置され、時刻設定要求に応じて、前記時刻情報の設定を行う設定手段を備えることを特徴とする請求項 1～9 のいずれか一つに記載の署名作成装置。

【請求項 1 1】 前記時刻認証機関に設置され、前記時計に対して自動的に校正をかける校正手段を備えることを特徴とする請求項 1～9 のいずれか一つに記載の署名作成装置。

【請求項 1 2】 共通鍵方式を用いてデジタル署名を作成する署名作成装置であって、

作成装置を特定するための装置 ID を平文に連結する連結手段と、

前記連結手段により作成された連結データ、および署名作成専用の共通鍵を用いて前記デジタル署名を作成する署名作成手段と、

を備えることを特徴とする署名作成装置。

【請求項 1 3】 時刻認証機関によってのみ時刻情報が設定される時計と、前記時刻情報および作成装置を特定するための装置 ID を平文に連結する連結手段と、前記連結手段により作成された連結データ、および署名作成専用の鍵を用いてデジタル署名を作成する署名作成手段とを備える署名作成装置により作成された前記デジタル署名に基づいて改竄の検証を行う署名検証装置であって、

前記デジタル署名が連結された前記平文を受信する受信手段と、

前記デジタル署名、前記平文、および署名検証専用の鍵を用いて、改竄を検

証する署名検証手段と、

を備えることを特徴とする署名検証装置。

【請求項 14】 鍵認証機関から、前記署名検証専用の鍵が暗号化された暗号情報の提供を受け、該暗号情報を復号することにより前記署名検証専用の鍵を生成する署名検証鍵生成手段を備えることを特徴とする請求項 13 に記載の署名検証装置。

【請求項 15】 時刻認証機関によってのみ時刻情報が設定される時計と、前記時刻情報および作成装置を特定するための装置 ID を平文に連結する連結手段と、

前記連結手段により作成された連結データ、および署名作成専用の鍵を用いてデジタル署名を作成する署名作成手段と、

前記デジタル署名が連結された前記平文を受信する受信手段と、

前記デジタル署名、前記平文、および署名検証専用の鍵を用いて、改竄を検証する署名検証手段と、

前記作成時に、前記時計、前記連結手段および前記署名作成手段における署名作成機能を有効にし、前記検証時に、前記受信手段および前記署名検証手段における署名検証機能を有効にする機能選択手段と、

を備えることを特徴とする署名装置。

【請求項 16】 下位装置としての機能と上位装置としての機能を切り替える切替手段と、

前記切替手段により上位装置としての機能に切り替えられ、かつ前記機能選択手段により前記署名検証機能が有効にされた場合に、前記下位装置であってかつ前記署名作成機能が有効にされた他の署名装置を特定するための装置 ID に基づいて、前記署名検証専用の鍵を生成する鍵生成手段と、

を備え、

前記署名作成専用の鍵と前記署名検証専用の鍵とは、共通鍵方式における共通鍵であり、前記署名検証手段は、前記鍵生成手段により生成された前記署名検証用の鍵を用いて、前記改竄を検証することを特徴とする請求項 15 に記載の署名装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、電子化情報の改竄を防止する署名作成装置および署名検証装置ならびに署名装置に関するものであり、特に、暗号化技術を用いたデジタル署名により署名日時、署名装置、署名者等の認証を行うことで改竄を効果的に防止する署名作成装置および署名検証装置ならびに署名装置に関するものである。

【0002】

紙ベースで処理されていたドキュメント、帳票等は、ペーパーレス化の要請から、徐々に電子化された電子化情報としてコンピュータにより処理されている。この種の電子化情報を扱う場合には、電子化情報を作成した本人になりすました第三者による改竄が行われる可能性がある。そこで、従来より、電子化情報に対する改竄が行われていないことを認証する技術として、暗号化技術を用いたデジタル署名技術が注目されている。特に、現在、飛躍的に普及しているイントラネット、インターネットを介して電子化情報をやりとりする場合に、デジタル署名技術は、セキュリティを確保するための技術として必須となりつつある。

【0003】

【従来の技術】

従来より、イントラネットやインターネットを介して電子化情報（以下、平文と称する）を送信する際、平文の内容が改竄されていないことを認証するために、平文を署名鍵を用いて暗号化してデジタル署名を作成した後、このデジタル署名を平文に添付したものを送信している。また、受信側においては、上記デジタル署名に基づいて、電子化情報が改竄されているか否かを検証している。このような、デジタル署名の作成／検証には、署名装置が用いられている。

【0004】

ここで、デジタル署名の作成／検証には、代表的な暗号化の方式である共通鍵方式または公開鍵方式が採用されている。この共通鍵方式は、作成側（送信側）と検証側（受信側）とで共通の鍵（共通鍵）を保有することに特徴があり、共通鍵方式の代表的なアルゴリズムとしては、周知のDES（Data Encryption St

andard) が業界の実質的な標準として用いられている。この共通鍵方式を用いた場合において、作成側の署名装置では、共通鍵を用いて平文を暗号化したものをデジタル署名として作成した後、平文にデジタル署名を添付したものをネットワーク等を介して送信する。

【0005】

そして、上記デジタル署名が添付された平文を受信すると、検証側の署名装置では、共通鍵を用いて上記平文を暗号化してデジタル署名を作成した後、このデジタル署名と、受信したデジタル署名とを比較し、この比較結果に基づいて、受信した平文が改竄されているか否かを検証する。すなわち、検証側の署名装置では、両デジタル署名が一致した場合、平文が改竄されていないことが検証され、両デジタル署名が一致しない場合、平文が改竄されていることが検証される。

【0006】

一方、上述した公開鍵方式は、暗号化する鍵と、復号化する鍵とが別々に存在する方式である。一方の鍵は、公開鍵と呼ばれ第三者に対して公開されており、他方の鍵は、プライベート鍵と呼ばれユーザ本人のみが保有している。この公開鍵方式は、公開鍵とプライベート鍵という二つの鍵を利用することで運用を行う方式であるため、公開鍵とプライベート鍵とがなければ暗号化および復号化ができない仕組みになっている。ここで、公開鍵方式の代表的なアルゴリズムとしては、周知のRSA (Rivest、Shamir、Adleman の3氏の頭文字) が用いられている。

【0007】

上記公開鍵方式を用いたデジタル署名において、作成者は、自身の公開鍵を第三者に公開するとともに、プライベート鍵を保有している。ここで、作成者の公開鍵が、作成者以外の第三者のいずれもが知り得る鍵であるのに対して、作成者のプライベート鍵は、作成者のみが知りうる鍵である。

【0008】

上述した公開鍵方式を用いた場合において、作成側の署名装置では、ハッシュ関数により、任意長のビット列からなる平文を固定長のビット列に圧縮(変換)

することでダイジェストを作成する。上記ハッシュ関数は、変換後のダイジェストから変換前の平文を導出することが数学的にほとんど不可能である、という一方向性を有する関数である。そして、作成側の署名装置では、作成者のプライベート鍵を用いて上記ダイジェストを暗号化したものをデジタル署名として作成した後、平文に上記デジタル署名を添付したものをネットワーク等を介して送信する。

【0009】

そして、上記デジタル署名が添付された平文を受信すると、検証側の署名装置では、作成者の公開鍵を用いてデジタル署名を復号し、この復号結果に基づいて、受信した平文が正当な作成者により作成されたものであるか否かを検証する。すなわち、受信したデジタル署名が作成者の公開鍵で復号できた場合、検証側の署名装置では、復号結果としてダイジェストが作成されるとともに、正当な作成側の署名装置（作成者）により、平文が作成されたことが検証される。一方、受信したデジタル署名が作成者の公開鍵で復号できなかった場合、検証側の署名装置では、受信した平文が、正当な作成者になりすました第三者により作成されたことが検証される。

【0010】

さらに、検証側の署名装置では、作成側の署名装置で用いられたものと同一のハッシュ関数により、受信した平文からダイジェストを作成した後、このダイジェストと、作成者の公開鍵により復号されたダイジェストとを比較することで、送信された平文が改竄されているか否かを検証する。すなわち、検証側の署名装置では、両ダイジェストが一致した場合、平文が改竄されていないことが検証され、両ダイジェストが一致しない場合、平文が改竄されていることが検証される。

【0011】

ここで、医療用のカルテ、税務帳票、議事録等のドキュメントにおいては、正当な権限を有する作成者が、後日問題が生じた場合に、日時を改竄して新規にドキュメントを作成するという、不正行為に対する防御が必要になる。このような防御にも、前述したデジタル署名技術が応用されている。すなわち、この場合

、には、署名装置の時計より日時情報を得て、これをタイムスタンプとして、上記ドキュメントが電子化された平文に付加したものに対して、デジタル署名を行うことにより、署名日時が正当であることの認証が可能となる。なお、タイムスタンプを用いた時間認証の詳細については、特開平 3-185551 号公報、特開平 7-254897 号公報および米国特許第 4458109 号公報を参照されたい。

【0012】

【発明が解決しようとする課題】

ところで、前述したように、従来の署名装置においては、平文にタイムスタンプを付加したものに対してデジタル署名することで署名日時の認証を行っている旨を述べた。しかしながら、作成者により時計の計時結果を容易に変更できるような装置である場合には、作成者が不正利用の目的で、タイムスタンプの内容（日時）を過去の日時に容易に改竄することで、署名日時の正当性が保証されなくなり、デジタル署名が法的に意味を持たなくなるという問題があった。

【0013】

また、共通鍵方式を用いた従来の署名装置においては、作成側と検証側とで共通鍵が共に用いられていることから、不正な検証者が正当な作成者に成りすまして、受信した平文に対してデジタル署名を行うことが可能となる。したがって、この場合には、デジタル署名を行った者の正当性を保証できないという問題が発生する。すなわち、この場合には、デジタル署名を行った者（装置）を特定することができないという問題が発生する。

【0014】

さらに、企業組織等においては、デジタル署名を行った者に関する情報（たとえば、役職名、氏名等）が重要な意味を持つ。このことから、企業組織等においては、職制変更が頻繁に行われるため、かかる変更に対応できる署名装置が要請されている。

【0015】

本発明は、上記に鑑みてなされたもので、日時の改竄を防止することができるとともに、デジタル署名を行った者、装置を特定することができ、しかも作成

者に関する情報の変更に対応できる署名作成装置および署名検証装置ならびに署名装置を提供することを目的とする。

【0016】

【課題を解決するための手段】

上記目的を達成するために、請求項1にかかる発明は、デジタル署名を作成する署名作成装置において、時刻認証機関によってのみ時刻情報が設定される時計（後述する実施の形態1および2の時計103に相当）と、前記時刻情報および作成装置を特定するための装置IDを平文に連結する連結手段（後述する実施の形態1、2の連結部102および連結部106に相当）と、前記連結手段により作成された連結データ、および署名作成専用の鍵を用いて前記デジタル署名を作成する署名作成手段（後述する実施の形態1の署名作成回路112、実施の形態2の署名作成回路702に相当）とを備えることを特徴とする。

【0017】

この請求項1にかかる発明によれば、時計の時刻情報は、時刻認証機関によってのみ設定されるため、第三者による不正な時刻の改竄が行われることがない。また、請求項1にかかる発明によれば、連結手段により、上記時刻情報および装置IDが平文に連結された後、署名作成手段により、連結データおよび署名作成専用の鍵に基づいてデジタル署名が作成される。このように、請求項1にかかる発明によれば、時計の時刻情報の設定を時刻認証機関以外で行えないようにするとともに、時刻情報および装置IDを含む連結データおよび署名専用の鍵を用いてデジタル署名を作成するようにしたので、日時の改竄を防止することができる。とともに、デジタル署名を作成した装置を特定することができる。

【0018】

また、請求項2にかかる発明は、請求項1に記載の署名作成装置において、前記連結手段（後述する実施の形態1、2の連結部109に相当）は、前記時刻情報および前記装置IDに加えて、デジタル署名を作成した者を特定するための個人特定情報（たとえば、氏名、職制）を前記平文に連結することを特徴とする。

【0019】

この請求項 2 にかかる発明によれば、連結手段により、時刻情報、装置 ID に加えて個人特定情報が平文に連結されると、署名作成手段によりデジタル署名が作成される。このように、請求項 2 にかかる発明によれば、個人特定情報を含む連結データを用いてデジタル署名を作成するようにしたので、検証側でデジタル署名の作成者を容易に特定することができるとともに、作成者に関する情報の変更に柔軟に対応することができる。

【0020】

また、請求項 3 にかかる発明は、前記個人特定情報を記憶する記憶手段と、前記記憶手段の記憶内容の更新を行う更新者が、正当な権限を有する者であるか否かを判断する判断手段（後述する実施の形態 1、2 の時計更新部 105 に相当）と、前記判断手段により前記更新者が正当な権限を有する者であると判断された場合にのみ、前記記憶手段の記憶内容を更新する更新手段（後述する実施の形態 1、2 の時計更新部 105 に相当）とを備えることを特徴とする。

【0021】

この請求項 3 にかかる発明によれば、判断手段により、記憶手段の記憶内容（個人特定情報）を更新する際の更新者が正当な権限を有する者であるか否かが判断され、正当な更新者が正当な権限を有する者であると判断された場合にのみ、更新手段により記憶内容が更新される。このように、請求項 3 にかかる発明によれば、判断手段を設けたことにより、個人特定情報を不正に更新する第三者を排除することができるため、セキュリティが向上する。

【0022】

また、請求項 4 にかかる発明は、請求項 1～3 のいずれか一つに記載の署名作成装置において、前記装置 ID は、書き換え不可能な記憶手段（後述する実施の形態 1、2 の装置 ID 記憶部 101 に相当）に記憶されていることを特徴とする。

【0023】

この請求項 4 にかかる発明によれば、装置 ID が書き換え不可能な記憶手段（たとえば、ワンタイム ROM）に記憶されているため、装置 ID の改竄を防止することができることから、セキュリティがさらに向上する。

【 0 0 2 4 】

また、請求項 5 にかかる発明は、請求項 1 ～ 4 のいずれか一つに記載の署名作成装置において、前記時計の動作状態を確認する確認手段（後述する実施の形態 1、2 のプロセッサに相当）を備え、前記署名作成手段は、前記確認手段により前記時計が正常に動作していることが確認された場合にのみ、前記デジタル署名を作成することを特徴とする。

【 0 0 2 5 】

この請求項 5 にかかる発明によれば、確認手段により時計が正常に動作していることが確認された場合にのみ、署名作成手段によりデジタル署名が作成されるようにしたので、時刻情報の信頼性が高水準に維持される。

【 0 0 2 6 】

また、請求項 6 にかかる発明は、請求項 5 に記載の署名作成装置において、前記署名作成手段は、前記確認手段により前記時計が正常に動作していないと確認された場合、前記署名作成専用の鍵の利用を停止し、前記時刻情報を含まない連結情報と前記署名作成専用の鍵以外の鍵とを用いて、デジタル署名を作成することを特徴とする。

【 0 0 2 7 】

この請求項 6 にかかる発明によれば、時計が故障等に起因して、正常に動作しない場合、すなわち、時刻情報を含む連結データに基づいてデジタル署名が作成できない場合に署名作成専用の鍵の利用を停止し、時刻情報を含まない連結情報と署名作成専用の鍵以外の鍵を用いてデジタル署名を作成できるようにしたので、汎用性が向上する。

【 0 0 2 8 】

また、請求項 7 にかかる発明は、請求項 5 または 6 に記載の署名作成装置において、前記確認手段は、前記時計の駆動電圧としきい値との比較結果に基づいて、前記時計の動作状態を確認することを特徴とする。

【 0 0 2 9 】

この請求項 7 にかかる発明によれば、確認手段により、駆動電圧としきい値との比較結果において、たとえば、時計の駆動電圧がしきい値電圧より低い場合に

、時計が正常動作していないことを確認するようにしたので、時刻情報の信頼性が高水準に維持される。

【0030】

また、請求項8にかかる発明は、請求項5または6に記載の署名作成装置において、前記確認手段は、一時点前の前記時計の計時結果と、現時点の計時結果との比較結果に基づいて、前記時計の動作状態を確認することを特徴とする。

【0031】

この請求項8にかかる発明によれば、確認手段により、一時点前の計時結果と現時点の計時結果との比較結果において、たとえば、両計時結果が一致した場合に、時計が停止していることを確認するようにしたので、時刻情報の信頼性が高水準に維持される。

【0032】

また、請求項9にかかる発明は、請求項5または6に記載の署名作成装置において、前記確認手段は、前記時計が正常動作している場合、フラグをオンにし、前記時計が正常動作していない場合、前記フラグをオフにし、前記署名作成手段は、前記フラグがオンにされている場合にのみ、前記デジタル署名を作成することを特徴とする。

【0033】

この請求項9にかかる発明によれば、確認手段によりフラグがオンにされている場合、すなわち、時計が正常動作している場合にのみ、署名作成手段によりデジタル署名を作成するようにしたので、時刻情報に関して信頼性が高いデジタル署名が作成される。

【0034】

また、請求項10にかかる発明は、請求項1～9のいずれか一つに記載の署名作成装置において、前記時刻認証機関に設置され、時刻設定要求に応じて、前記時刻情報の設定を行う設定手段を備えることを特徴とする。

【0035】

この請求項10にかかる発明によれば、時刻設定要求に応じて、時刻認証機関に設置された設定手段により時計の時刻設定が行われるようにしたので、第三者

による不正な時刻の改竄が効果的に防止される。

【0036】

また、請求項 11 にかかる発明は、請求項 1～9 のいずれか一つに記載の署名作成装置において、前記時刻認証機関に設置され、前記時計に対して自動的に校正をかける校正手段を備えることを特徴とする。

【0037】

この請求項 11 にかかる発明によれば、校正手段により自動的に時計が校正されるため、時計から得られる時刻情報の精度が高水準に維持される。

【0038】

また、請求項 12 にかかる発明は、共通鍵方式を用いてデジタル署名を作成する署名作成装置であって、作成装置を特定するための装置 ID を平文に連結する連結手段（後述する実施の形態 1 の連結部 102 に相当）と、前記連結手段により作成された連結データ、および署名作成専用の共通鍵を用いて前記デジタル署名を作成する署名作成手段（後述する実施の形態 1 の署名作成回路 112 に相当）とを備えることを特徴とする。

【0039】

この請求項 12 にかかる発明によれば、共通鍵方式において、作成装置を特定するための装置 ID を含む連結データおよび署名専用の鍵を用いてデジタル署名を作成するようにしたので、検証側において、デジタル署名を作成した装置を特定することができる。

【0040】

また、請求項 13 にかかる発明は、時刻認証機関によってのみ時刻情報が設定される時計と、前記時刻情報および作成装置を特定するための装置 ID を平文に連結する連結手段と、前記連結手段により作成された連結データ、および署名作成専用の鍵を用いてデジタル署名を作成する署名作成手段とを備える署名作成装置により作成された前記デジタル署名に基づいて改竄の検証を行う署名検証装置であって、前記デジタル署名が連結された前記平文を受信する受信手段（後述する実施の形態 1 の分離部 501、実施の形態 2 の分離部 801 に相当）と、前記デジタル署名、前記平文、および署名検証専用の鍵を用いて、改竄を検

証する署名検証手段（後述する実施の形態 1 の署名作成回路 504 および比較部 505、実施の形態 2 の圧縮回路 802、復号回路 803 および比較部 805 に相当）とを備えることを特徴とする。

【0041】

この請求項 13 にかかる発明によれば、受信手段によりデジタル署名が連結された平文が受信されると、署名検証手段は、デジタル署名、平文および署名検証専用の鍵を用いて、改竄を検証する。このように請求項 13 にかかる発明によれば、認証された時刻情報および装置 ID を含む連結データに基づいてデジタル署名を検証しているため、日時の改竄を防止することができるとともに、デジタル署名を作成した装置を特定することができる。

【0042】

また、請求項 14 にかかる発明は、請求項 13 に記載の署名検証装置において、鍵認証機関から、前記署名検証専用の鍵が暗号化された暗号情報の提供を受け、該暗号情報を復号することにより前記署名検証専用の鍵を生成する署名検証鍵生成手段を備えることを特徴とする。

【0043】

この請求項 14 にかかる発明によれば、鍵認証機関という信頼性が高い機関より、暗号情報の提供を受け、この暗号情報を署名検証鍵生成手段により復号することで署名検証専用の鍵を生成するようにしたので、装置におけるセキュリティを極めて高くすることができる。

【0044】

また、請求項 15 にかかる発明は、時刻認証機関によってのみ時刻情報が設定される時計（後述する実施の形態 3 の時計 903 に相当）と、前記時刻情報および作成装置を特定するための装置 ID を平文に連結する連結手段（後述する実施の形態 3 のプロセッサ 901 に相当）と、前記連結手段により作成された連結データ、および署名作成専用の鍵を用いてデジタル署名を作成する署名作成手段（後述する実施の形態 3 の署名作成／検証回路 905 に相当）と、前記デジタル署名が連結された前記平文を受信する受信手段（後述する実施の形態 3 の入出力バッファメモリ 902 に相当）と、前記デジタル署名、前記平文、および署

名検証専用の鍵を用いて、改竄を検証する署名検証手段（後述する実施の形態 3 の署名作成／検証回路 905 に相当）と、前記作成時に、前記時計、前記連結手段および前記署名作成手段における署名作成機能を有効にし、前記検証時に、前記受信手段および前記署名検証手段における署名検証機能を有効にする機能選択手段（後述する実施の形態 3 のプロセッサ 901 に相当）とを備えることを特徴とする。

【0045】

この請求項 15 にかかる発明によれば、一つの装置に署名作成機能と署名検証機能を持たせることができる。すなわち、請求項 15 にかかる発明によれば、機能選択手段により署名作成機能が有効にされると、当該装置が、署名作成装置として機能し、また機能選択手段により署名検証機能が有効にされると、当該装置が、署名検証装置として機能するようにしたので、汎用性を向上させることができる。

【0046】

また、請求項 16 にかかる発明は、請求項 15 に記載の署名装置において、下位装置としての機能と上位装置としての機能を切り替える切替手段（後述する実施の形態 3 のプロセッサ 901 に相当（後述する実施の形態 1 のプロセッサに相当））と、前記切替手段により上位装置としての機能に切り替えられ、かつ前記機能選択手段により前記署名検証機能が有効にされた場合に、前記下位装置であってかつ前記署名作成機能が有効にされた他の署名装置を特定するための装置 ID に基づいて、前記署名検証専用の鍵を生成する鍵生成手段（後述する実施の形態 3 のプロセッサ 901 に相当（後述する実施の形態 1 の署名検証鍵生成部 503 に相当））とを備え、前記署名作成専用の鍵と前記署名検証専用の鍵とは、共通鍵方式における共通鍵であり、前記署名検証手段は、前記鍵生成手段により生成された前記署名検証用の鍵を用いて、前記改竄を検証することを特徴とする。

【0047】

この請求項 16 にかかる発明によれば、切替手段により上位装置としての機能に切り替えられ、かつ機能選択手段により署名検証機能が有効にされると、当該署名装置は、署名検証装置として機能する。また、他の署名装置が下位装置とし

ての機能を備え、かつ署名作成装置として機能している状態においてデジタル署名が作成されると、上記署名検証機能を備える上位装置においては、鍵生成手段により下位装置の装置IDに基づき署名検証専用の鍵が生成される。これにより、上位装置の署名検証手段は、上記署名検証専用の鍵を用いて、下位装置からのデジタル署名に基づいて改竄を検証する。このように請求項16にかかる発明によれば、下位装置が複数台ある場合であっても、上位装置では下位装置の装置IDを管理すればよいと、複数の下位装置のそれぞれの共通鍵を管理する場合のように厳重な管理を行う必要がない。

【0048】

【発明の実施の形態】

以下、図面を参照して本発明にかかる署名作成装置および署名検証装置ならびに署名装置の実施の形態1～3について詳細に説明する。

【0049】

(実施の形態1)

図1は、本発明の実施の形態1の構成を示すブロック図である。図1には、前述した共通鍵方式を用いてデジタル署名を作成する署名作成装置100、および作成されたデジタル署名に基づいて検証を行う署名検証装置500が図示されている。この図において、署名作成装置100は、デジタル署名の作成側に設置されたコンピュータ200に接続されており、電子化された平文A（図3（a）参照）を入力データとして、デジタル署名を作成する装置である。実際には、署名作成装置100は、携帯可能なカード型の装置であり、コンピュータ200のカードスロットに挿入接続されている。この署名作成装置100の詳細については後述する。

【0050】

コンピュータ200は、イントラネット、ローカルエリアネットワーク、インターネット等のネットワーク300に接続されており、署名作成装置100からの署名済みデータM（図3（f）参照）を送信する機能を備えている。コンピュータ400は、デジタル署名の検証側に設置されており、ネットワーク300に接続されている。このコンピュータ400は、コンピュータ200から送信さ

れた署名済みデータMを受信する機能を備えている。署名検証装置500は、署名済みデータMの正当性を検証する装置である。この署名検証装置500は、署名作成装置100と同様にして、携帯可能なカード型の装置であり、コンピュータ400のカードスロットに挿入接続されている。コンピュータ600は、CA (Certificate Authority) センターに設置されており、後述する署名作成装置100の時計103における時刻設定、認証を行う。上記CAセンターは、時刻認証に関してユーザから絶対的な信頼を受けた時刻認証機関である。また、CAセンターは、デジタル署名、暗号化／復号化に用いられる鍵の認証に関して、ユーザから絶対的な信頼を受けており、公開鍵証明書の発行等を行う鍵認証機関である。

【0051】

また、作成側の署名作成装置100の機能としては、下位装置としての機能と、上位装置としての機能とがある。同様にして、検証側の署名検証装置500の機能としては、下位装置としての機能と、上位装置としての機能とがある。ここで、これらの下位装置と上位装置との関係について図2(a)および(b)を参照して説明する。図2(a)に示した下位装置100Aは、下位装置ID (Identification number : 識別符号)、署名作成鍵 K_{s1} および署名検証鍵 K_{c1} を保持している。上記下位装置IDは、下位装置100Aを特定するためのIDである。署名作成鍵 K_{s1} は、デジタル署名の作成専用の鍵であり、他の目的に利用できないようにインプリメントされている。この署名作成鍵 K_{s1} には、作成専用の鍵であることを表す作成属性データ S_d が付加されている。署名検証鍵 K_{c1} は、デジタル署名の検証専用の鍵であり、他の目的に利用できないようにインプリメントされている。この署名検証鍵 K_{c1} には、検証専用の鍵であることを表す検証属性データ C_d が付加されている。

【0052】

一方、図2(b)に示した上位装置100Bは、上述した作成属性データ S_d と同様の作成属性データ S_d' が付加された署名作成鍵 K_{s1}' 、検証属性データ C_d と同様の検証属性データ C_d' が付加された署名検証鍵 K_{c1}' を保持している。また、上位装置100Bは、下位装置IDを用いて署名作成鍵 K_{s1}' を署名

検証鍵 K_{s1} ”に変換する機能を備えている。たとえば、署名検証鍵 K_{s1} ”は、下位装置IDが署名作成鍵 K_{s1} ’で暗号化されたものであり、デジタル署名の検証専用の鍵である。この署名検証鍵 K_{s1} ”と下位装置100Aの署名作成鍵 K_{s1} とは、対をなしており、共通鍵方式における共通鍵である。したがって、下位装置100Aにおいて署名作成鍵 K_{s1} を用いて作成されたデジタル署名は、上位装置100Bにおいて生成された署名検証鍵 K_{s1} ”によってのみ検証が可能である。

【0053】

さらに、上位装置100Bは、下位装置IDを用いて署名検証鍵 K_{c1} ’を署名作成鍵 K_{c1} ”に変換する機能を備えており、この署名作成鍵 K_{c1} ”は、下位装置IDが署名検証鍵 K_{c1} ’で暗号化されたものであり、デジタル署名の作成専用の鍵である。この署名作成鍵 K_{c1} ”と下位装置100Aの署名検証鍵 K_{c1} とは、対をなしており、共通鍵方式における共通鍵である。したがって、上位装置100Bにおいて署名作成鍵 K_{c1} ”を用いて作成されたデジタル署名は、下位装置100Aの署名検証鍵 K_{c1} によってのみ検証可能である。

【0054】

このように、上述した方法を用いることにより、下位装置100Aが複数台ある場合であっても、上位装置100Bでは下位装置IDを管理すればよいので、複数の下位装置100Aのそれぞれの共通鍵を管理する場合のように厳重な管理を行う必要がない。また、上述した方法を用いることにより、管理共通鍵を一方の共通鍵（署名作成鍵 K_{s1} 、署名検証鍵 K_{s1} ”）でデジタル署名の作成が可能な装置を下位装置100Aのみとすることができるため、上記一方の共通鍵を用いてデジタル署名を作成した装置の特定が可能となる。同様に、他方の共通鍵（署名作成鍵 K_{c1} ”、署名検証鍵 K_{c1} ）でデジタル署名の作成が可能な装置を上位装置100Bのみとすることができるため、上記他方の共通鍵を用いてデジタル署名を作成した装置の特定が可能となる。

【0055】

ここで、図1に示した署名作成装置100は、上述した下位装置100A（図2（a）参照）または上位装置100B（図2（b）参照）としての機能を備え

ている。一方、署名検証装置 500 は、署名作成装置 100 が下位装置 100A としての機能を備えている場合、上位装置 100B としての機能を備える。この場合とは逆に署名作成装置 100 が上位装置 100B としての機能を備えている場合、署名検証装置 500 は、下位装置 100A としての機能を備える。

【0056】

署名作成装置 100 において、装置 ID 記憶部 101 は、装置を特定するための装置 ID・B (図 3 (b) 参照) を記憶する。この装置 ID 記憶部 101 は、ワンタイム ROM (Read Only Memory) 等の書き換え不可能な記憶デバイスからなる。したがって、署名作成装置 100 においては、装置 ID・B を外部から変更できないようになっている。連結部 102 は、コンピュータ 200 から入力される平文 A (図 3 (a) 参照) と、装置 ID 記憶部 101 から読み出された装置 ID・B (図 3 (b) 参照) とを連結する。

【0057】

時計 103 は、デジタル署名の作成の日時の認証に用いられる、日付、時刻等の時間に関する時刻情報を生成する。この時計 103 には、駆動用の電池 104 が内蔵されている。この電池 104 は、一次電池または充電可能な二次電池である。時計更新部 105 は、時計 103 における時刻の更新 (設定) 時に用いられるものであり、コンピュータ 200 およびネットワーク 300 を介してコンピュータ 600 にアクセスすることで、時刻設定の要求を行う。すなわち、時計 103 は、CA センターに設置されたコンピュータ 600 以外からは、時刻の設定ができないようになっている。また、時計更新部 105 とコンピュータ 600 とにおいては、署名作成装置 100 のプライベート鍵および公開鍵を用いてデジタル署名の作成、検証が行われる。

【0058】

連結部 106 は、連結部 102 から出力されるデータ (平文 A + 装置 ID・B) に、時計 103 からの時刻情報をタイムスタンプ C (図 3 (c) 参照) として連結する。個人特定情報記憶部 107 は、デジタル署名を作成する者を特定するための個人特定情報 D (図 3 (d) 参照) を記憶する。この個人特定情報 D としては、氏名や職制等が挙げられる。個人特定情報更新部 108 は、外部から入

力される個人特定情報に基づいて、個人特定情報記憶部 107 に記憶されている個人特定情報 D を更新（入力、変更）する。この個人特定情報更新部 108 を用いて個人特定情報 D を更新（入力、変更）できる者は、正当な権限を有する者に限定されている。したがって、署名作成装置 100 においては、たとえば、パスワード入力によるセキュリティ機能により、第三者の不正更新（入力、変更）を防止している。連結部 109 は、連結部 106 から出力されるデータ（平文 A + 装置 ID・B + タイムスタンプ C）に個人特定情報 D（図 3（d）参照）を連結し、これを署名対象データ E とする。

【0059】

鍵記憶部 110 は、署名作成装置 100 が上位装置 100B（図 2（b）参照）としての機能を備える場合、前述した検証属性データ C_d' が付加された署名検証鍵 K_{c1}' を記憶する。また、鍵記憶部 110 は、署名作成装置 100 が下位装置 100A（図 2（a）参照）としての機能を備える場合、前述した作成属性データ S_d が付加された署名作成鍵 K_{s1} を記憶する。署名作成鍵生成部 111 は、署名作成装置 100 が上位装置 100B としての機能を備える場合に用いられ、図 2（b）を参照して説明したように、下位装置 ID と署名検証鍵 K_{c1}' とから署名作成鍵 K_{c1}'' を生成し、これを署名作成回路 112 へ出力する。なお、署名作成装置 100 が下位装置 100A としての機能を備える場合には、署名作成鍵生成部 111 の機能が停止され、同図二点鎖線で示したように署名作成鍵 K_{s1} （図 2（a）参照）が署名作成回路 112 に入力される。

【0060】

署名作成回路 112 は、共通鍵方式における DES を用いることで、署名対象データ E（図 3（d）参照）を署名作成鍵 K_{c1}'' （または署名作成鍵 K_{s1} ）で暗号化し、MAC（Message Authentication Code）と呼ばれる認証子（デジタル署名）を生成する。この認証子は、署名 L（図 3（e）参照）として出力される。ここで、署名作成回路 112 においては、署名作成装置 100 が上位装置 100B としての機能を備えている場合、署名作成鍵 K_{c1}'' が共通鍵として用いられ、署名作成装置 100 が下位装置 100A としての機能を備えている場合、署名作成鍵 K_{s1} が共通鍵として用いられる。連結部 113 は、署名対象データ E に

署名Lを連結し、これを署名済みデータM（図3（f）参照）としてコンピュータ200へ送出する。コンピュータ200は、ネットワーク300を介して上記署名済みデータMをコンピュータ400へ送出する。

【0061】

署名検証装置500において、分離部501は、コンピュータ400により受信された署名済みデータM（図4（a）参照）を、図4（b）に示したように署名対象データEと署名Lとに分離する。鍵記憶部502は、署名検証装置500が上位装置100B（図2（b）参照）としての機能を備える場合、前述した作成属性データ S_d' が付加された署名作成鍵 K_{s1}' を記憶する。また、鍵記憶部502は、署名検証装置500が下位装置100A（図2（a）参照）としての機能を備える場合、前述した検証属性データ C_d が付加された署名検証鍵 K_{c1} を記憶する。署名検証鍵生成部503は、署名検証装置500が上位装置100Bとしての機能を備える場合に用いられ、図2（b）を参照して説明したように、下位装置ID（この場合、署名作成装置100の装置ID・B）と署名作成鍵 K_{s1}' とから署名検証鍵 K_{s1}'' を生成し、これを署名作成回路504へ出力する。なお、署名検証装置500が下位装置100Aとしての機能を備える場合には、署名検証鍵生成部503の機能が停止され、同図二点鎖線で示したように署名検証鍵 K_{c1} （図2（a）参照）が署名作成回路504に入力される。

【0062】

署名作成回路504は、署名作成装置100の署名作成回路112と同様の機能を備えており、分離部501により分離された署名対象データE（図4（b）参照）を署名検証鍵 K_{s1}'' （または署名検証鍵 K_{c1} ）で暗号化し、MACと呼ばれる認証子（デジタル署名）を生成する。この認証子は、署名N（図4（c）参照）として出力される。ここで、署名作成回路504においては、署名検証装置500が上位装置100Bとしての機能を備えている場合には、署名検証鍵 K_{s1}'' が、下位装置100Aとしての機能を備える署名作成装置100における署名作成鍵 K_{s1} との共通鍵として用いられる。また、署名検証装置500が下位装置100Aとしての機能を備えている場合には、署名検証鍵 K_{c1} が、上位装置100Bとしての機能を備える署名作成装置100における署名作成鍵 K_{c1}'' との

共通鍵として用いられる。

【0063】

比較部505は、分離部501により分離された署名L（図4（b）参照）と、署名作成回路504により作成された署名N（図4（c）参照）とを比較することで、署名対象データEが改竄されているか否かの検証を行う。すなわち、比較部505は、両者が一致した場合、検証結果を改竄無しとし、両者が一致しない場合、検証結果を改竄有りとする。

【0064】

つぎに、上述した実施の形態1の動作について図5に示したフローチャートを参照しつつ説明する。署名作成装置100において電源がONにされると、図示しないプロセッサは、図5に示したステップSA1へ進み、時計103が使用可能状態にあるか否かを示すフラグをチェックした後、ステップSA2へ進む。このフラグがONである場合には、時計103が使用可能な状態（デジタル署名の作成が可能な状態）にあることを示しており、フラグがOFFである場合には、時計103が使用不可能な状態（デジタル署名の作成が不可能な状態）にあることを示している。

【0065】

ステップSA2では、プロセッサは、フラグがONであるか否かを判断する。ここで、フラグがOFFである場合、プロセッサは、デジタル署名の作成が不可能であるものと判断し、ステップSA2の判断結果を「No」として、処理を終了する。一方、ステップSA2の判断結果が「Yes」である場合、プロセッサは、ステップSA3へ進み、電池104の電圧をチェックした後、ステップSA4へ進む。

【0066】

ステップSA4では、プロセッサは、チェックした電圧がしきい値以上であるか否かを判断する。ここで、しきい値は、時計103の正常な動作を保証する最低電圧である。ステップSA4の判断結果が「No」である場合、プロセッサは、時計103が使用不可能な状態、すなわち、タイムスタンプCの正常性が保証されない状態にあるものとして、ステップSA8へ進み、フラグをOFFにした

後、処理を終了する。一方、ステップSA4の判断結果が「Yes」である場合、プロセッサは、ステップSA5へ進み、時計103が動作しているか否かを確認した後、ステップSA6へ進む。具体的には、プロセッサは、時計103の計時結果を取得した後、所定時間経過後に再び計時結果を取得し、両計時結果を比較することにより、時計103が動作しているか否かを確認する。

【0067】

ステップSA6では、プロセッサは、時計103が正常に動作しているか否かを、ステップSA5の確認結果に基づいて判断する。すなわち、後に取得した計時結果が、先に取得した計時結果より進んでいる場合には、プロセッサは、時計103が正常に動作しているものと判断する。他方、両計時結果が一致している場合には、プロセッサは、時計103が停止しているものと判断する。ステップSA6の判断結果が「No」である場合、プロセッサは、ステップSA8へ進み、フラグをOFFにした後、処理を終了する。一方、ステップSA6の判断結果が「Yes」である場合、プロセッサは、ステップSA7へ進み、連結情報付き署名処理を実行する。

【0068】

ここで、上記連結情報とは、図3(d)に示したように平文Aに連結された情報(装置ID・B、タイムスタンプC、個人特定情報D)をいう。また、以下に説明する連結情報付き署名処理において用いられる鍵(署名作成鍵 K_{s1} 、署名作成鍵 K_{s1}' 、署名検証鍵 K_{s1}'' 、署名検証鍵 K_{c1} 、署名検証鍵 K_{c1}' 、署名作成鍵 K_{c1}'' ：図2(a)および(b)参照)は、連結情報付き署名処理において専用に用いられる鍵である。したがって、これらの鍵は、連結情報が連結されていない平文Aに対するデジタル署名の作成／検証や、平文Aのみに関する暗号化／復号化に用いられる鍵とは別のものである。

【0069】

つぎに、連結情報付き署名処理について詳述する。はじめに、署名作成装置100が下位装置100A(図2(a)参照)としての機能を備えるとともに、署名検証装置500が上位装置100B(図2(b)参照)としての機能を備える場合について説明する。コンピュータ200より平文Aが連結部102に入力さ

れると、平文Aには、連結部102、連結部106および連結部109により図3(b)～図3(d)に示したように、装置ID・B、タイムスタンプCおよび個人特定情報Dが順次、連結される。そして、署名作成回路112および連結部113には、署名対象データE(図3(d)参照)がそれぞれ入力される。

【0070】

これにより、署名作成回路112では、図3(e)に示したように署名対象データEが署名作成鍵 K_{s1} により暗号化されることで、署名Lが作成され、連結部113では、図3(f)に示したように、署名対象データEに上記署名Lが連結されることで、署名済みデータMが作成される。そして、上記署名済みデータMは、コンピュータ200により、ネットワーク300へ送出されることで、コンピュータ400に受信された後、署名検証装置500の分離部501に入力される。そして、署名済みデータM(図4(a)参照)は、図4(b)に示したように、分離部501により署名対象データEと署名Lとに分離される。

【0071】

これにより、署名作成回路504では、図4(c)に示したように、分離された署名対象データEが署名検証鍵生成部503により生成された署名検証鍵 K_{s1} ”により暗号化されることで、署名Nが作成される。そして、比較部505は、分離された他方の署名Lと、署名作成回路504により作成された署名Nとを比較することで、署名対象データEが改竄されているか否かの検証を行う。ここで、比較部505は、両者が一致した場合、検証結果を改竄無しとし、両者が一致しない場合、検証結果を改竄有りとする。

【0072】

なお、署名作成装置100が上位装置100B(図2(b)参照)としての機能を備えるとともに、署名検証装置500が下位装置100A(図2(a)参照)としての機能を備える場合、署名作成装置100の署名作成回路112では、前述した署名作成鍵 K_{s1} に代えて、署名作成鍵生成部111により生成された署名作成鍵 K_{c1} ”が用いられる。一方、署名検証装置500の署名作成回路504では、前述した署名検証鍵 K_{s1} ”に代えて署名検証鍵 K_{c1} が用いられる。

【0073】

さて、前述においては、署名作成装置 100 における時計 103 の時刻設定が時刻認証機関である CA センターのコンピュータ 600 によってのみ行い得ることを述べた。以下、時計 103 の時刻設定について図 6 を参照しつつ説明する。この時刻設定は、電池 104 の交換や、電池 104 の充電が行われることにより、前述したフラグが OFF である場合、署名作成装置 100 の時計更新部 105 により実行される。この場合、コンピュータ 200 から時刻設定のコマンドが入力されると、図 6 に示したステップ SR1 では、署名作成装置 100 の時計更新部 105 は、コンピュータ 200 およびネットワーク 300 を経由して CA センターのコンピュータ 600 にアクセスし、時刻設定を要求する。これにより、ステップ SR2 では、コンピュータ 600 は、署名作成装置 100 の装置 ID を要求する。そして、この要求を受けた時計更新部 105 は、ステップ SR3 で装置 ID をコンピュータ 600 へ送出する。

【0074】

つぎのステップ SR4 では、コンピュータ 600 は、正確な日付け、時刻に関する時刻設定情報を送出する。この際、コンピュータ 600 は、上記時刻設定情報を、公開鍵方式における署名作成装置 100 のプライベート鍵により暗号化することでデジタル署名を作成し、このデジタル署名を時刻設定情報に連結したものを送出する。そして、デジタル署名付きの時刻設定情報を受信すると、時計更新部 105 は、公開鍵を用いてデジタル署名を検証する。この検証の結果、改竄が無い場合、ステップ SR5 では、時計更新部 105 は、上記時刻設定情報に基づいて時計 103 を校正することで、正確な時刻設定を行った後、時刻設定の応答をコンピュータ 600 に対して行う。なお、この応答時においては、署名作成装置 100 のプライベート鍵を用いてデジタル署名を作成し、これをコンピュータ 600 へ送信するようにしてもよい。

【0075】

そして、上記応答を受け取ったコンピュータ 600 は、ステップ SR6 で、時計更新部 105 に対して、校正後の時計 103 の時刻情報を要求する。この要求を受け取った時計更新部 105 は、ステップ SR7 において時計 103 の時刻情報をコンピュータ 600 へ送出する。この際、時計更新部 105 は、上記時刻情

報を、署名作成装置 100 のプライベート鍵により暗号化することでデジタル署名を作成し、このデジタル署名を時刻情報に連結したものを送出する。そして、デジタル署名付きの時刻情報を受信すると、コンピュータ 600 は、公開鍵を用いてデジタル署名を検証する。この検証の結果、改竄が無い場合、ステップ S R 8 では、コンピュータ 600 により、時刻設定完了の通知が時計更新部 105 へ出される。これにより、署名作成装置 100 において、前述したフラグが OFF から ON にされた後、一連の時刻設定が完了する。

【0076】

なお、上述においては、署名作成装置 100 側からの時刻設定要求に応じて、コンピュータ 600 が時刻設定を行う場合について説明したが、コンピュータ 600 から署名作成装置 100（時計更新部 105）に定期的にアクセスして、時計 103 を自動的に校正するようにしてもよい。この場合の動作について、図 7 を参照して詳述する。図 7 に示したステップ S Q 1 では、コンピュータ 600 は、ネットワーク 300 およびコンピュータ 200 を経由して署名作成装置 100 の時計更新部 105 にアクセスし、署名作成装置 100 の装置 ID を要求する。そして、この要求を受けた時計更新部 105 は、ステップ S Q 2 で装置 ID をコンピュータ 600 へ送出する。

【0077】

つぎのステップ S Q 3 では、コンピュータ 600 は、時計更新部 105 に対して、現時点における時計 103 の時刻情報を要求する。この要求を受け取った時計更新部 105 は、ステップ S Q 4 で時計 103 の時刻情報をコンピュータ 600 へ送出する。この際、時計更新部 105 は、上記時刻情報を、プライベート鍵により暗号化することでデジタル署名を作成し、このデジタル署名を時刻情報に連結したものを送出する。そして、デジタル署名付きの時刻情報を受信すると、コンピュータ 600 は、公開鍵を用いてデジタル署名を検証する。この検証の結果、改竄が無い場合、コンピュータ 600 は、上記時刻情報の誤差の有無を、正確な時刻情報との比較結果に基づいて検証し、誤差がない場合、いずれの処理も行わない。

【0078】

ここで、誤差がある場合、ステップSQ5では、コンピュータ600は、正確な日付け、時刻に関する時刻設定情報を送出する。この際、コンピュータ600は、上記時刻設定情報を、署名作成装置100のプライベート鍵により暗号化することでデジタル署名を作成し、このデジタル署名を時刻設定情報に連結したものを送出する。そして、デジタル署名付きの時刻設定情報を受信すると、時計更新部105は、公開鍵を用いてデジタル署名を検証する。この検証の結果、改竄が無い場合、ステップSQ6では、時計更新部105は、上記時刻設定情報に基づいて時計103を校正することで、正確な時刻設定を行った後、時刻設定の応答をコンピュータ600に対して行う。なお、この応答時には、署名作成装置100のプライベート鍵を用いてデジタル署名を作成し、これをコンピュータ600へ送信するようにしてもよい。

【0079】

そして、応答を受け取ったコンピュータ600は、ステップSQ7において時計更新部105に対して校正後の時計103の時刻情報を要求する。つぎのステップSQ8では、時計更新部105は、校正後の時刻情報をコンピュータ600へ送出する。この際、時計更新部105は、上記時刻情報を、プライベート鍵により暗号化することでデジタル署名を作成し、このデジタル署名を時刻情報に連結したものを送出する。そして、デジタル署名付きの時刻情報を受信すると、コンピュータ600は、公開鍵を用いてデジタル署名を検証する。この検証の結果、改竄が無い場合、ステップSQ9では、コンピュータ600により、時刻設定完了の通知が時計更新部105へ出されることで、一連の時刻情報の自動校正が完了する。以後、コンピュータ600は、定期的に署名作成装置100の時計更新部105へアクセスすることで、時計103を自動的に校正する。このような自動校正が行われることにより、時計103の時刻情報（タイムスタンプC）の精度が高水準に維持される。

【0080】

なお、上述した実施の形態1においては、図1に示した署名検証鍵生成部503により、署名作成鍵 K_{s1}' および下位装置ID情報から署名検証鍵 K_{s1}'' を生成する例について説明したが、同図2点鎖線で示したように、CAセンターに設

置されたコンピュータ600からの暗号情報 C_r および署名検証装置500の固有鍵 K_r から署名検証鍵 K_{s1} ”を生成するようにしてもよい。すなわち、この場合、コンピュータ600においては、署名検証装置500の固有鍵 K_r を用いて、署名検証鍵 K_{s1} ”を暗号化することで、暗号情報 C_r を生成する。

【0081】

そして、コンピュータ600から上記暗号情報 C_r が送出されると、暗号情報 C_r は、ネットワーク300およびコンピュータ400を経由して、署名検証鍵生成部503に入力される。これにより、署名検証鍵生成部503は、暗号情報 C_r を固有鍵 K_r を用いて復号することで、署名検証鍵 K_{s1} ”を生成する。以下、上述した動作と同様にして、署名作成回路504では、上記署名検証鍵 K_{s1} ”に基づいて署名Nを作成する。このような構成によれば、高度の信頼性を有するCAセンターに設置されたコンピュータ600から暗号情報 C_r を受け取り、この暗号情報 C_r を復号することで署名検証鍵 K_{s1} ”を生成するようにしたので、署名検証装置500におけるセキュリティを極めて高くすることができる。

【0082】

また、上述した実施の形態1においては、連結情報を構成するものとして、装置ID・B、タイムスタンプCおよび個人特定情報Dという3つ情報を例に挙げたがこれに限られるものではない。すなわち、連結情報としては、上記3つの情報のうち、1つの情報のみ、または少なくとも2つの情報の組み合わせであってもよい。たとえば、ここで述べている連結情報の例としては、(a)項～(d)項が挙げられる。

- (a) 装置ID・BおよびタイムスタンプCからなる連結情報
- (b) 装置ID・Bのみからなる連結情報
- (c) タイムスタンプCのみからなる連結情報
- (d) 装置ID・Bおよび個人特定情報Dからなる連結情報

【0083】

上記(a)項～(d)項のうち、(a)項の連結情報および(c)項の連結情報は、いずれもタイムスタンプCを含む情報であり、一方、(b)項の連結情報および(d)項の連結情報は、タイムスタンプCを含まない情報である。このよ

うに（a）項～（d）項のそれぞれの連結情報が連結された平文Aに基づいて、署名を作成する場合には、署名作成回路112において、それぞれの連結情報に対応する都合4種類の署名作成用の鍵を用いればよい。これら4種類の鍵は、鍵記憶部110に記憶させてもよく、また、署名作成鍵生成部111により作成するようにしてもよい。

【0084】

これに関連して、上述した実施の形態1においては、図5を参照して説明したように、電池104の電圧がしきい値より低い場合や、時計103が正常動作していない場合のように、時計103からのタイムスタンプC（時刻情報）を用いることができない場合に、連結情報付き署名処理を実行しない例について説明した。しかしながら、このような場合には、プロセッサの制御により、上述した（a）項や（c）項のタイムスタンプCを含む連結情報用の鍵の利用を停止するとともに、上述した（b）項や（d）項の連結情報のようにタイムスタンプCを含まない連結情報用の鍵を利用することで、（b）項または（d）項の連結情報に基づいて署名を作成すればよい。

【0085】

以上説明したように、上述した実施の形態1によれば、時計103の時刻情報の設定をCAセンターのコンピュータ600以外で行えないようにするとともに、平文Aに連結情報（装置ID・B、タイムスタンプC、個人特定情報D）を連結したのに対して、デジタル署名を行うようにし、かつ連結情報付きの署名専用の鍵を用いてデジタル署名を行うようにしたので、日時の改竄を防止することができるとともに、デジタル署名を行った者、装置を特定することができ、作成者を容易に特定することができる。また、実施の形態1によれば、個人特定情報更新部108により個人特定情報Dを容易に変更可能としたので、職制変更等にも柔軟に対応できる。

【0086】

（実施の形態2）

図8は、本発明の実施の形態2の構成を示すブロック図である。この図において、図1の各部に対応する部分にはそれぞれ同一の符号を付けその説明を省略す

る。図 8 には、実施の形態 1 における共通鍵方式に代えて、公開鍵方式を用いてデジタル署名を作成する署名作成装置 700、および作成されたデジタル署名に基づいて検証を行う署名検証装置 800 が図示されている。署名作成装置 700 においては、公開鍵方式によるデジタル署名の作成／検証が行われるため、作成者（署名作成装置 700）のプライベート鍵である署名作成鍵 K_{s2} が用いられており、他方、署名検証装置 800 においては、作成者（署名作成装置 700）の公開鍵である署名検証鍵 K_{c2} が用いられている。ここで、署名作成鍵 K_{s2} および署名検証鍵 K_{c2} は、実施の形態 1 の場合と同様にして、連結情報付き署名の作成および検証専用の鍵であり、他の目的には使用できないようになっている。

【0087】

署名作成装置 700 は、署名作成装置 100（図 1 参照）と同様にしてカード型の装置としてコンピュータ 200 のカードスロットに挿入・接続されている。この署名作成装置 700 は、平文 A（図 9（a）参照）に連結された連結情報（装置 ID・B、タイムスタンプ C および個人特定情報 D（図 9（b）、（c）および（d）参照））に関する署名（デジタル署名）I（図 9（g）参照）を作成する。ここで、署名作成装置 700 においては、図 1 に示した鍵記憶部 110、署名作成鍵生成部 111、署名作成回路 112 および連結部 113 に代えて、圧縮回路 701、署名作成回路 702、鍵記憶部 703 および連結部 704 が設けられている。

【0088】

上記鍵記憶部 703 には、署名作成鍵 K_{s2} が記憶されており、圧縮回路 701 は、連結部 109 より入力される署名対象データ E（図 9（d）参照）を前述したハッシュ関数によって圧縮したハッシュ値 F（図 9（e）参照）に、ビット列からなる Pad 値 G（図 9（f）参照）を連結することで、ダイジェスト H を作成する。このダイジェスト H は、固定長のビット列からなる。署名作成回路 702 は、図 9（g）に示したように、上記ダイジェスト H を署名作成鍵 K_{s2} により暗号化することで、署名（デジタル署名）I を作成する。連結部 704 は、図 9（h）に示したように、連結部 109 からの署名対象データ E と、署名作成回

路 702 により作成された署名 I とを連結し、これを署名済みデータ J としてコンピュータ 200 へ送出する。

【0089】

一方、署名検証装置 800 は、署名検証装置 500（図 1 参照）と同様にして、カード型の装置としてコンピュータ 400 のカードスロットに挿入・接続されている。この署名検証装置 800 は、コンピュータ 400 により受信された署名済みデータ J（図 10（a）参照）に基づいて署名 I を検証する装置である。署名検証装置 800 において、分離部 801 は、図 10（b）に示したように、署名済みデータ J を署名対象データ E と署名 I とに分離する。圧縮回路 802 は、署名作成装置 700 の圧縮回路 701 と同様の機能を備えている。

【0090】

すなわち、圧縮回路 802 は、圧縮回路 701 において用いられたものと同じハッシュ関数を用いて、署名対象データ E を圧縮した結果（ハッシュ値）に Pad 値を連結することで、図 10（c）に示したダイジェスト K を作成する。復号回路 803 は、図 10（d）に示したように署名 I を、鍵記憶部 804 に記憶された署名検証鍵 K_{c2} により復号することで、ダイジェスト H を作成する。比較部 805 は、上記ダイジェスト K とダイジェスト H とを比較することにより、署名対象データ E の改竄の有無を検証する。すなわち比較部 805 は、ダイジェスト K とダイジェスト H とが一致する場合には、検証結果を改竄無しとし、両者が一致しない場合には、検証結果を改竄有りとする。

【0091】

つぎに、上述した実施の形態 2 の動作について説明する。ここで、実施の形態 2 における基本的な動作は、図 5 に示したステップ SA1～ステップ SA6 およびステップ SA8、図 6 に示したステップ SR1～ステップ SR8、ならびに図 7 に示したステップ SQ1～ステップ SQ9 と同様であるため、これらの説明を省略する。したがって、ここでは、実施の形態 2 におけるステップ SA7 の連結情報付き署名処理について説明する。

【0092】

この連結情報付き署名処理において、コンピュータ 200 より平文 A が署名作

成装置 700 の連結部 102 に入力されると、平文 A には、連結部 102、連結部 106 および連結部 109 により図 9 (b) ~ 図 9 (d) に示したように、装置 ID・B、タイムスタンプ C および個人特定情報 D が順次、連結される。そして、圧縮回路 701 および連結部 704 には、署名対象データ E (図 9 (d) 参照) がそれぞれ入力される。

【0093】

これにより、圧縮回路 701 では、署名対象データ E がハッシュ関数により圧縮されたハッシュ値 F (図 9 (e) 参照) に Pad 値 G が連結され、ダイジェスト H (図 9 (f) 参照) が作成される。署名作成回路 702 では、図 9 (g) に示したようにダイジェスト H が署名作成鍵 K_{s2} により暗号化されることで、署名 I が作成され、連結部 704 では、図 9 (h) に示したように、署名対象データ E に署名 I が連結されることで、署名済みデータ J が作成される。そして、この署名済みデータ J は、コンピュータ 200 により、ネットワーク 300 へ送出されることで、コンピュータ 400 に受信された後、署名検証装置 800 の分離部 801 に入力される。そして、署名済みデータ J (図 10 (a) 参照) は、図 10 (b) に示したように、分離部 801 により署名対象データ E と署名 I とに分離される。

【0094】

これにより、圧縮回路 802 では、図 10 (c) に示したように、ハッシュ関数に基づいて署名対象データ E からダイジェスト K が作成される。一方、復号回路 803 では、図 10 (d) に示したように、分離された署名 I が署名検証鍵 K_{c2} により復号されることで、ダイジェスト H が作成される。比較部 805 は、ダイジェスト K とダイジェスト H とを比較し、両者が一致した場合、検証結果を改竄無しとし、両者が一致しない場合、検証結果を改竄有りとする。

【0095】

以上説明したように、上述した実施の形態 2 によれば、前述した実施の形態 1 と同様にして、日時の改竄を防止することができるとともに、デジタル署名を行った者、装置を特定することができ、作成者を容易に特定することができる。さらに、実施の形態 2 によれば、個人特定情報更新部 108 により個人特定情報

Dを容易に変更可能としたので、職制変更等にも柔軟に対応できる。

【0096】

(実施の形態3)

さて、前述した実施の形態1および2では、署名作成装置と署名検証装置とを別々に設けた例について説明したが、署名作成機能および署名検証機能の双方を備える署名装置を、作成側および検証側にそれぞれ設けるようにしてもよい。この場合、作成側の署名装置では、署名作成機能を選択するようにし、検証側の署名装置では、署名検証機能を選択するようにすればよい。以下、この場合を実施の形態3として説明する。

【0097】

図11は、本発明の実施の形態3の構成を示すブロック図である。この図において、図1および図8の各部に対応する部分には同一の符号を付ける。この図において、署名装置900Aは、署名作成／検証機能に加えて、暗号化／復号化機能を備えており、コンピュータ200に接続されている。署名装置900Aにおいて、署名作成／検証機能は、図1に示した署名作成装置100および署名検証装置500、ならびに図8に示した署名作成装置700および署名検証装置800と同様の機能である。署名装置900Bは、署名装置900Aと同一の機能を備えており、コンピュータ400に接続されている。ここで、署名装置900Aおよび署名装置900Bは、カード型の装置であり、コンピュータ200およびコンピュータ400のそれぞれのカードスロットに挿入・接続されている。

【0098】

ここで、図12を参照して上述した署名装置900Aの構成について説明する。この図において、プロセッサ901は、装置各部を制御するものであり、図1に示した時計更新部105、個人特定情報更新部108、署名作成鍵生成部111および署名検証鍵生成部503と同様の機能を備えている。このプロセッサ901の動作の詳細については、フローチャートを参照して後述する。入出力バッファメモリ902は、コンピュータ200との間で入出力されるデータを一時的に記憶するメモリである。時計903は、電池904により駆動され、図1に示した時計103と同様にして、時刻情報を生成する。この時計903は、実施の

形態 1 および 2 と同様にして、コンピュータ 600（図 11 参照）のみにより時刻設定が可能である。電池 904 は、一次電池または充電可能な二次電池である。

【0099】

署名作成／検証回路 905 は、前述した実施の形態 1 または 2 における共通鍵方式または公開鍵方式を用いた署名作成／検証機能を備えている。具体的には、署名作成／検証回路 905 は、図 1 に示した署名作成装置 100 および署名検証装置 500 の機能と、図 8 に示した署名作成装置 700 および署名検証装置 800 の機能とを備えている。鍵記憶部 906 は、署名作成／検証回路 905 において用いられる署名作成鍵、署名検証鍵（共通鍵、公開鍵、プライベート鍵）を記憶する。これら署名作成鍵および署名検証鍵は、前述した実施の形態 1 および 2 において説明したものと同様の鍵である。

【0100】

ここで、上記署名作成鍵および署名検証鍵は、前述した連結情報付き署名処理専用の鍵であるが、鍵記憶部 906 には、上記専用の鍵の他に、連結情報が連結されていない平文 A（図 3（a）参照）のみに対して、署名作成／検証を行う処理（以下、平文署名処理と称する）のための鍵が記憶されている。さらに、鍵記憶部 906 には、後述する暗号／復号回路 909 において用いられる暗号鍵、復号鍵を記憶している。つまり、署名装置 900A は、連結情報付き署名処理、平文署名処理および暗号／復号処理という三つの処理を行えるようになっている。

【0101】

個人特定情報記憶部 907 は、個人特定情報記憶部 107（図 1 参照）と同様にして、個人特定情報を記憶する。装置 ID 記憶部 908 は、装置 ID 記憶部 101（図 1 参照）と同様にして、署名装置 900A を特定するための装置 ID を記憶する。暗号／復号回路 909 は、鍵記憶部 906 に記憶されている暗号鍵／復号鍵により、暗号／復号処理を行う。なお、署名装置 900B の構成は、上述した署名装置 900A の構成と同様である。ただし、署名装置 900B において、装置 ID 記憶部 908 には、署名装置 900B を特定するための装置 ID が記憶されている。

【0102】

つぎに、上述した実施の形態3の動作について図13に示したフローチャートを参照しつつ説明する。この場合、図11に示した署名装置900Aは、署名作成の機能に用いられるものとし、他方の署名装置900Bは、署名検証に用いられるものとする。図13に示したステップSB1では、署名装置900Aのプロセッサ901は、コンピュータ200からのコマンド入力に基づいて、連結情報付き署名処理、平文署名処理、暗号／復号処理のうちいずれかの処理を選択する。この場合、連結情報付き署名処理が選択されたものとする、プロセッサ901は、ステップSB4へ進む。なお、平文署名処理が選択された場合、プロセッサ901は、ステップSB3へ進み、署名作成／検証回路905を制御することで、コンピュータ200より入力される平文（図3（a）参照）に対して署名作成を行う平文署名処理を実行する。また、暗号／復号処理が選択された場合、プロセッサ901は、ステップSB2へ進み、暗号／復号回路909を制御することで、暗号／復号処理を実行する。

【0103】

ステップSB4では、実施の形態1と同様にして、プロセッサ901は、時計903が使用可能状態にあるか否かを示すフラグをチェックした後、ステップSB5へ進む。このフラグがONである場合には、時計903が使用可能な状態（デジタル署名の作成が可能な状態）にあることを示しており、フラグがOFFである場合には、時計903が使用不可能な状態（デジタル署名の作成が不可能な状態）にあることを示している。

【0104】

ステップSB5では、プロセッサ901は、フラグがONであるか否かを判断する。ここで、フラグがOFFである場合、プロセッサ901は、デジタル署名の作成が不可能であるものと判断し、ステップSB5の判断結果を「No」として、処理を終了する。一方、ステップSB5の判断結果が「Yes」である場合、プロセッサ901は、ステップSB6へ進み、電池904の電圧をチェックした後、ステップSB7へ進む。

【0105】

ステップSB7では、プロセッサ901は、チェックした電圧がしきい値以上であるか否かを判断し、この判断結果が「No」である場合、ステップSB11へ進み、フラグをOFFにした後、処理を終了する。一方、ステップSB7の判断結果が「Yes」である場合、プロセッサ901は、ステップSB8へ進み、時計903が動作しているか否かを確認した後、ステップSB9へ進む。ステップSB9では、プロセッサ901は、時計903が正常に動作しているか否かを、ステップSB8の確認結果に基づいて判断し、この判断結果が「No」である場合、ステップSB11へ進み、フラグをOFFにした後、処理を終了する。一方、ステップSB9の判断結果が「Yes」である場合、プロセッサ901は、ステップSB10へ進み、図14に示した連結情報付き署名処理を実行する。

【0106】

図14に示した連結情報付き署名処理において、ステップSC1では、コンピュータ200（作成者）は、コマンド入力により、署名装置900Aに対して署名処理で用いられる鍵を設定する。この場合、署名装置900Aが署名作成機能を有する装置として用いられるため、コンピュータ200は、署名作成用の鍵を、署名装置900Aの署名作成／検証回路905および鍵記憶部906に設定する。したがって、この場合、上記署名作成／検証回路905は、署名作成回路として用いられる。

【0107】

つぎのステップSC2では、コンピュータ200は、署名装置900Aに対して署名すべき、データ（平文A（図3（a）参照））の入力を開始した後、ステップSC3へ進む。ここで、上記データの量が非常に多い場合には、データを複数分割することで、数回に分けて入力が行われる。ステップSC3では、コンピュータ200は、上記データの入力が完了したか否かを判断し、この判断結果が「No」である場合、ステップSC2へ戻る。そして、データの入力が完了すると、コンピュータ200は、ステップSC3の判断結果を「Yes」とし、ステップSC4へ進む。ステップSC4では、コンピュータ200は、署名装置900Aの機能（署名作成機能または署名検証機能）を選択する。

【0108】

この場合、署名作成機能が選択されると、ステップSC5では、コンピュータ200は、署名作成コマンドの入力を行う。この署名作成コマンドが署名装置900Aのプロセッサ901に入力されると、プロセッサ901は、上述した実施の形態1（または実施の形態2）における署名作成装置100（または署名作成装置700）と同様にして、連結情報付き署名の作成処理を実行する。これにより、図11に示した署名装置900Aからは、署名済みデータM（図3（f）参照）（または、署名済みデータJ（図9（h）参照））がネットワーク300を介して、コンピュータ400へ送出される。

【0109】

そして、上記署名済みデータM（または署名済みデータJ）を受信すると、コンピュータ400は、図14に示したステップSC1では、鍵を設定する。この場合、署名装置900Bが署名検証機能を有する装置として用いられるため、コンピュータ400は、署名検証用の鍵を、署名装置900Bの署名作成／検証回路905および鍵記憶部906に設定する。したがって、この場合、署名作成／検証回路905は、署名検証回路として用いられる。

【0110】

つぎのステップSC2では、コンピュータ400は、署名装置900Bに対して検証すべき、データ（署名済みデータMまたは署名済みデータJ）の入力を開始した後、ステップSC3へ進む。ステップSC3では、コンピュータ400は、上記データの入力が完了したか否かを判断し、この判断結果が「No」である場合、ステップSC2へ戻る。そして、データの入力が完了すると、コンピュータ400は、ステップSC3の判断結果を「Yes」とし、ステップSC4へ進む。ステップSC4では、コンピュータ400は、署名装置900Bの機能（署名作成機能または署名検証機能）を選択する。この場合、署名検証機能が選択されると、ステップSC5では、コンピュータ400は、署名検証コマンドの入力を行う。

【0111】

署名検証コマンドが署名装置900Bのプロセッサ901に入力されると、プロセッサ901は、上述した実施の形態1（または実施の形態2）における署名

検証装置 500（または署名検証装置 800）と同様にして、連結情報付き署名の検証処理を実行する。なお、署名装置 900B においては、図 13 に示したステップ SB3 では、署名装置 900A において平文署名が行われたデータに対する検証が行われ、ステップ SB2 では、署名装置 900A において暗号化されたデータに対する復号が行われる。

【0112】

以上説明したように、上述した実施の形態 3 によれば、署名装置 900A および署名装置 900B に、連結情報付き署名処理、平文署名処理および暗号／復号処理という三つの処理のうち、いずれかの処理を選択して実行するようにしたので、汎用性が向上する。特に、実施の形態 3 においては、時計 903 が故障したときに、連結情報付き署名処理に代えて平文署名処理を行うことができる。また、上述した実施の形態 3 によれば、コンピュータ 200 およびコンピュータ 400 からのコマンド（署名作成コマンド、署名検証コマンド）入力により、署名装置 900A および署名装置 900B の機能を選択できるようにしたので、汎用性を向上させることができるとともに、インタフェースで共通部分（図 14 参照）があるため、実施の形態 1、2 の場合に比してファームウェアのサイズを小さくすることができる。

【0113】

以上本発明の実施の形態 1～3 について図面を参照して詳述してきたが、具体的な構成例はこの実施の形態に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等があっても本発明に含まれる。たとえば、実施の形態 1 においては、図 1 に示したように、作成側の署名作成装置 100 が 1 台、検証側の署名検証装置 500 が 1 台という 1：1 の構成例について説明したが、作成側の署名作成装置 100 が n 台に対して、検証側の署名検証装置 500 を 1 台という n：1 の構成としてもよい。

【0114】

このような構成の場合には、n 台の署名作成装置 100 において、それぞれユニークな共通鍵（署名作成鍵）、または一つの共通鍵（署名作成鍵）を共有して用いる場合が考えられる。作成側でユニークな共通鍵を用いた場合には、署名検

証装置 500 において n 個の共通鍵（署名検証鍵）を使い分ける必要があるが、セキュリティが向上する。一方、作成側で一つの共通鍵（署名作成鍵）を共有した場合には、署名検証装置 500 において一つの共通鍵（署名検証鍵）を用いればよい。よいため、鍵管理が容易となる。

【0115】

また、実施の形態 1 においては、図 6 および図 7 を参照して説明したように、署名作成装置 100 とコンピュータ 600 との間で時刻設定に関する情報の送信／受信に際して、公開鍵方式を用いたデジタル署名を行う例について説明したが、共通鍵方式を用いたデジタル署名を行うようにしてもよい。この時刻設定に関して、署名作成装置 100 が n 台ある場合には、装置毎に異なるプライベート鍵（または共通鍵）を用いるようにすればよい。なお、この場合には、装置間で共通なプライベート鍵（または共通鍵）を共有するようにしてもよい。

【0116】

また、実施の形態 3 において、同一の装置（署名装置 900A）により署名作成／検証を行うようにしてもよい。この場合には、署名装置 900A のプロセッサ 901 により検証結果を出す前に、署名済みデータ M（または署名済みデータ J）から得られる装置 ID と、署名装置 900A の装置 ID 記憶部 908 に記憶されている装置 ID とを比較し、この比較結果が一致した場合にのみ、署名済みデータ M（または署名済みデータ J）に対する検証を行うようにしてもよい。なお、上記比較結果が不一致である場合には、署名済みデータ M（または署名済みデータ J）が署名装置 900A 以外の装置により作成されたことを意味している。最後に、実施の形態 1～3 のうちいずれか二つまたは三つ組み合わせた構成も、本発明に含まれる。

【0117】

【発明の効果】

以上説明したように、請求項 1 にかかる発明によれば、時計の時刻情報の設定を時刻認証機関以外で行えないようにするとともに、時刻情報および装置 ID を含む連結データおよび署名専用の鍵を用いてデジタル署名を作成するようにしたので、日時の改竄を防止することができるとともに、デジタル署名を作成し

た装置を特定することができるという効果を奏する。

【0118】

また、請求項2にかかる発明によれば、個人特定情報を含む連結データを用いてデジタル署名を作成するようにしたので、検証側でデジタル署名の作成者を容易に特定することができるとともに、作成者に関する情報の変更に対応することができるという効果を奏する。

【0119】

また、請求項3にかかる発明によれば、判断手段を設けたことにより、個人特定情報を不正に更新する第三者を排除することができるため、セキュリティが向上するという効果を奏する。

【0120】

また、請求項4にかかる発明によれば、装置IDが書き換え不可能な記憶手段（たとえば、ワンタイムROM）に記憶されているため、装置IDの改竄を防止することができることから、セキュリティがさらに向上するという効果を奏する。

【0121】

また、請求項5にかかる発明によれば、確認手段により時計が正常に動作していることが確認された場合にのみ、署名作成手段によりデジタル署名が作成されるようにしたので、時刻情報の信頼性が高水準に維持されるという効果を奏する。

【0122】

また、請求項6にかかる発明によれば、時計が故障等に起因して、正常に動作しない場合、すなわち、時刻情報を含む連結データに基づいてデジタル署名が作成できない場合に署名作成専用の鍵の利用を停止し、時刻情報を含まない連結情報と署名作成専用の鍵以外の鍵を用いてデジタル署名を作成できるようにしたので、汎用性が向上するという効果を奏する。

【0123】

また、請求項7にかかる発明によれば、確認手段により、駆動電圧としきい値との比較結果において、たとえば、時計の駆動電圧がしきい値電圧より低い場合

に、時計が正常動作していないことを確認するようにしたので、時刻情報の信頼性が高水準に維持されるという効果を奏する。

【0124】

また、請求項8にかかる発明によれば、確認手段により、一時点前の計時結果と現時点の計時結果との比較結果において、たとえば、両計時結果が一致した場合に、時計が停止していることを確認するようにしたので、時刻情報の信頼性が高水準に維持されるという効果を奏する。

【0125】

また、請求項9にかかる発明によれば、確認手段によりフラグがオンにされている場合、すなわち、時計が正常動作している場合にのみ、署名作成手段によりデジタル署名を作成するようにしたので、時刻情報に関して信頼性が高いデジタル署名が作成されるという効果を奏する。

【0126】

また、請求項10にかかる発明によれば、時刻設定要求に応じて、時刻認証機関に設置された設定手段により時計の時刻設定が行われるようにしたので、第三者による不正な時刻の改竄を効果的に防止することができるという効果を奏する。

【0127】

また、請求項11にかかる発明によれば、校正手段により自動的に時計が校正されるため、時計から得られる時刻情報の精度が高水準に維持されるという効果を奏する。

【0128】

また、請求項12にかかる発明によれば、共通鍵方式において、作成装置を特定するための装置IDを含む連結データおよび署名専用の鍵を用いてデジタル署名を作成するようにしたので、検証側において、デジタル署名を作成した装置を特定することができるという効果を奏する。

【0129】

また、請求項13にかかる発明によれば、認証された時刻情報および装置IDを含む連結データに基づいてデジタル署名を検証しているため、日時の改竄を

防止することができるとともに、デジタル署名を作成した装置を特定することができるという効果を奏する。

【0 1 3 0】

また、請求項 1 4 にかかる発明によれば、鍵認証機関という信頼性が高い機関より、暗号情報の提供を受け、この暗号情報を署名検証鍵生成手段により復号することで署名検証専用の鍵を生成するようにしたので、装置におけるセキュリティを極めて高くすることができるという効果を奏する。

【0 1 3 1】

また、請求項 1 5 にかかる発明によれば、機能選択手段により署名作成機能が有効にされると、当該装置が、署名作成装置として機能し、また機能選択手段により署名検証機能が有効にされると、当該装置が、署名検証装置として機能するようにしたので、汎用性を向上させることができるという効果を奏する。

【0 1 3 2】

また、請求項 1 6 にかかる発明によれば、下位装置が複数台ある場合であっても、上位装置では下位装置の装置 ID を管理すればよいと、複数の下位装置のそれぞれの共通鍵を管理する場合のように厳重な管理を行う必要がないという効果を奏する。

【図面の簡単な説明】

【図 1】

本発明にかかる実施の形態 1 の構成を示すブロック図である。

【図 2】

同実施の形態 1 における下位装置 1 0 0 A と上位装置 1 0 0 B との関係を説明する図である。

【図 3】

同実施の形態 1 におけるデータ遷移を示す図である。

【図 4】

同実施の形態 1 におけるデータ遷移を示す図である。

【図 5】

同実施の形態 1 の動作を説明するフローチャートである。

【図 6】

同実施の形態 1 における時刻設定シーケンスを示す図である。

【図 7】

同実施の形態 1 における時刻設定シーケンスを示す図である。

【図 8】

本発明にかかる実施の形態 2 の構成を示すブロック図である。

【図 9】

同実施の形態 2 におけるデータ遷移を示す図である。

【図 1 0】

同実施の形態 2 におけるデータ遷移を示す図である。

【図 1 1】

本発明にかかる実施の形態 3 の構成を示すブロック図である。

【図 1 2】

図 1 1 に示した署名装置 9 0 0 A (9 0 0 B) の構成を示すブロック図である。

【図 1 3】

同実施の形態 3 の動作を説明するフローチャートである。

【図 1 4】

同実施の形態 3 における連結情報付き署名処理を説明するフローチャートである。

【符号の説明】

- 1 0 0 署名作成装置
- 1 0 1 装置 I D 記憶部
- 1 0 2 連結部
- 1 0 3 時計
- 1 0 5 時計更新部
- 1 0 6 連結部
- 1 0 7 個人特定情報記憶部
- 1 0 8 個人特定情報更新部

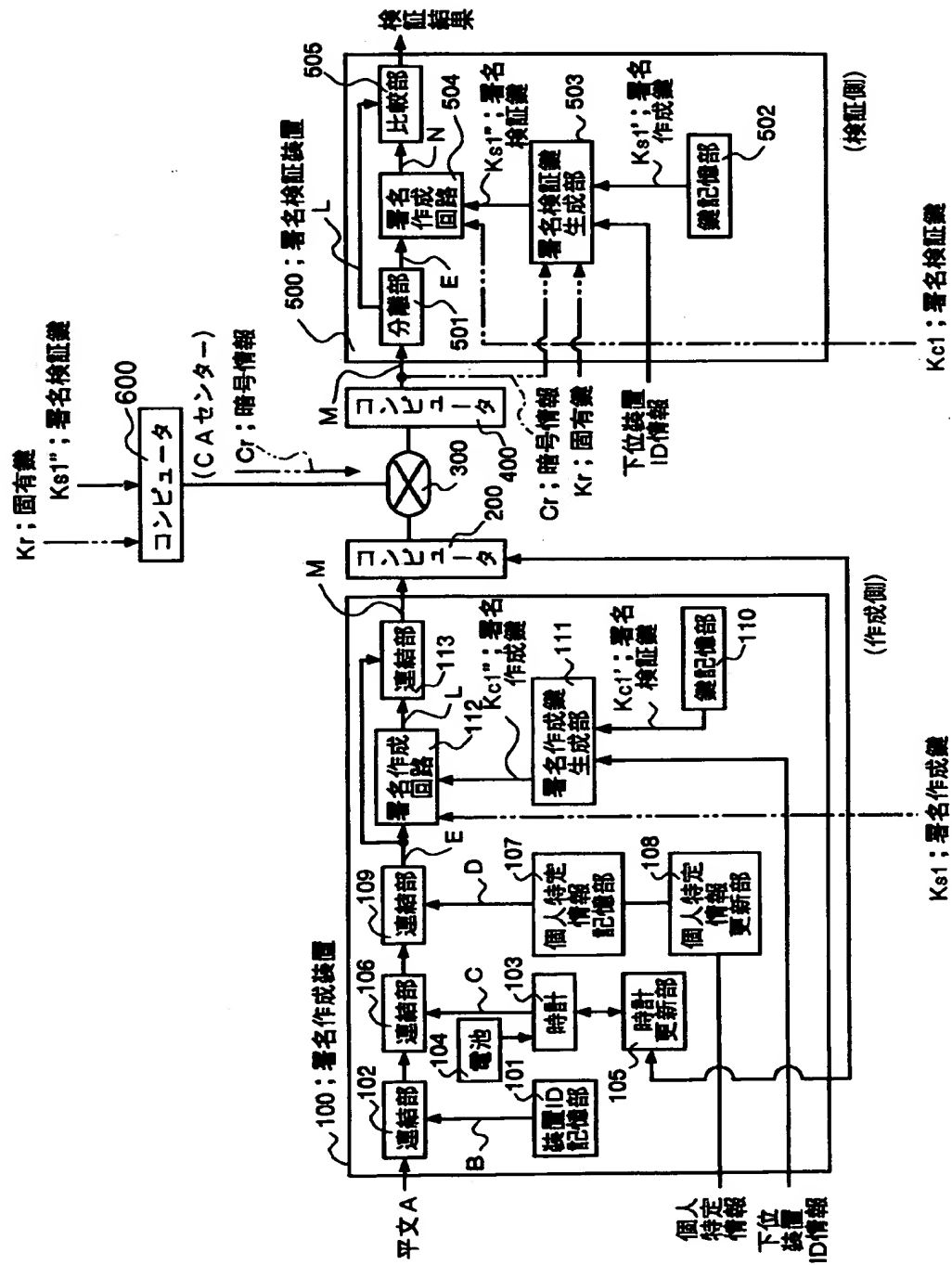
1 0 9 連結部
1 1 1 署名作成鍵生成部
1 1 2 署名作成回路
2 0 0 コンピュータ
4 0 0 コンピュータ
5 0 0 署名検証装置
5 0 3 署名検証鍵生成部
5 0 4 署名作成回路
5 0 5 比較部
6 0 0 コンピュータ
1 0 0 A 下位装置
1 0 0 B 上位装置
7 0 0 署名作成装置
7 0 2 署名作成回路
8 0 0 署名検証装置
8 0 3 復号回路
8 0 5 比較部
9 0 0 A 署名装置
9 0 0 B 署名装置
9 0 1 プロセッサ
9 0 3 時計
9 0 5 署名作成／検証回路
9 0 7 個人特定情報記憶部
9 0 8 装置 I D 記憶部

【書類名】

図面

【図 1】

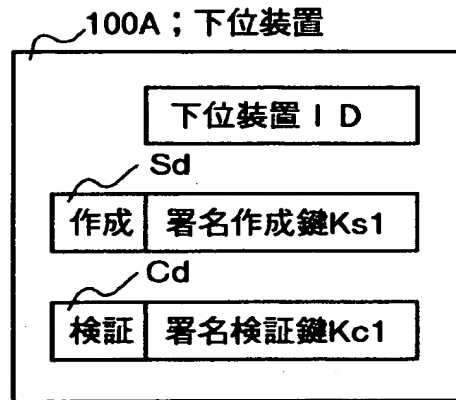
実施の形態 1 の構成を示すブロック図



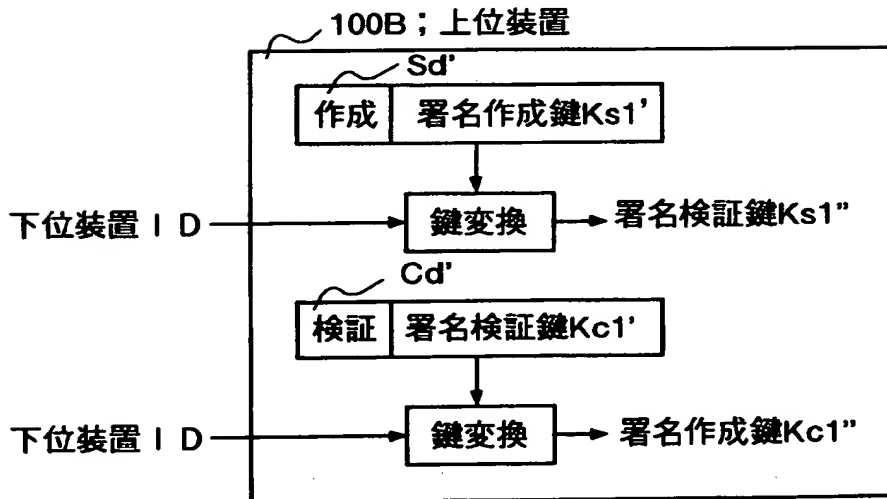
【図 2】

実施の形態 1 における下位装置 100A と上位装置 100B との
関係を説明する図

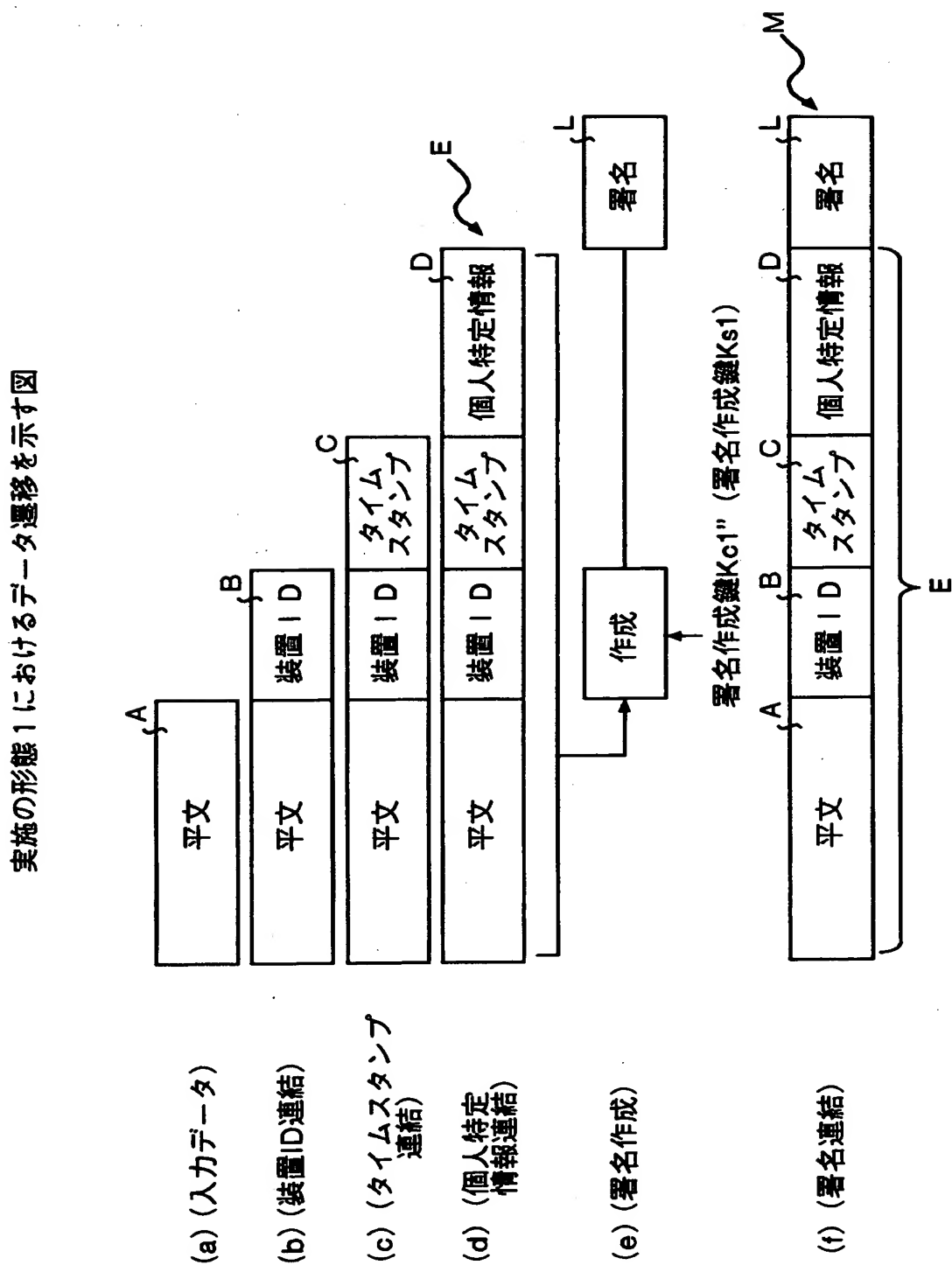
(a)



(b)

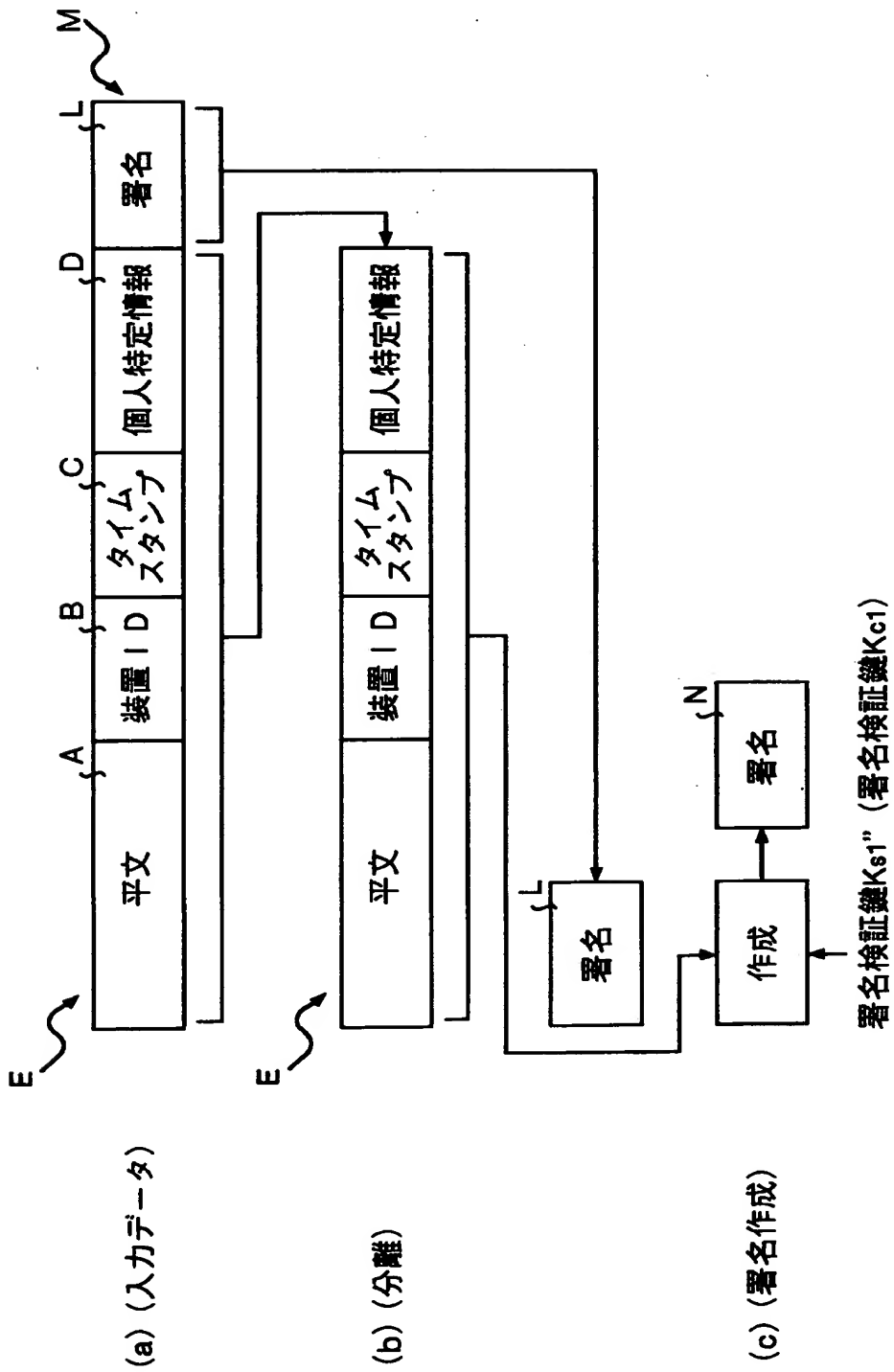


【図 3】



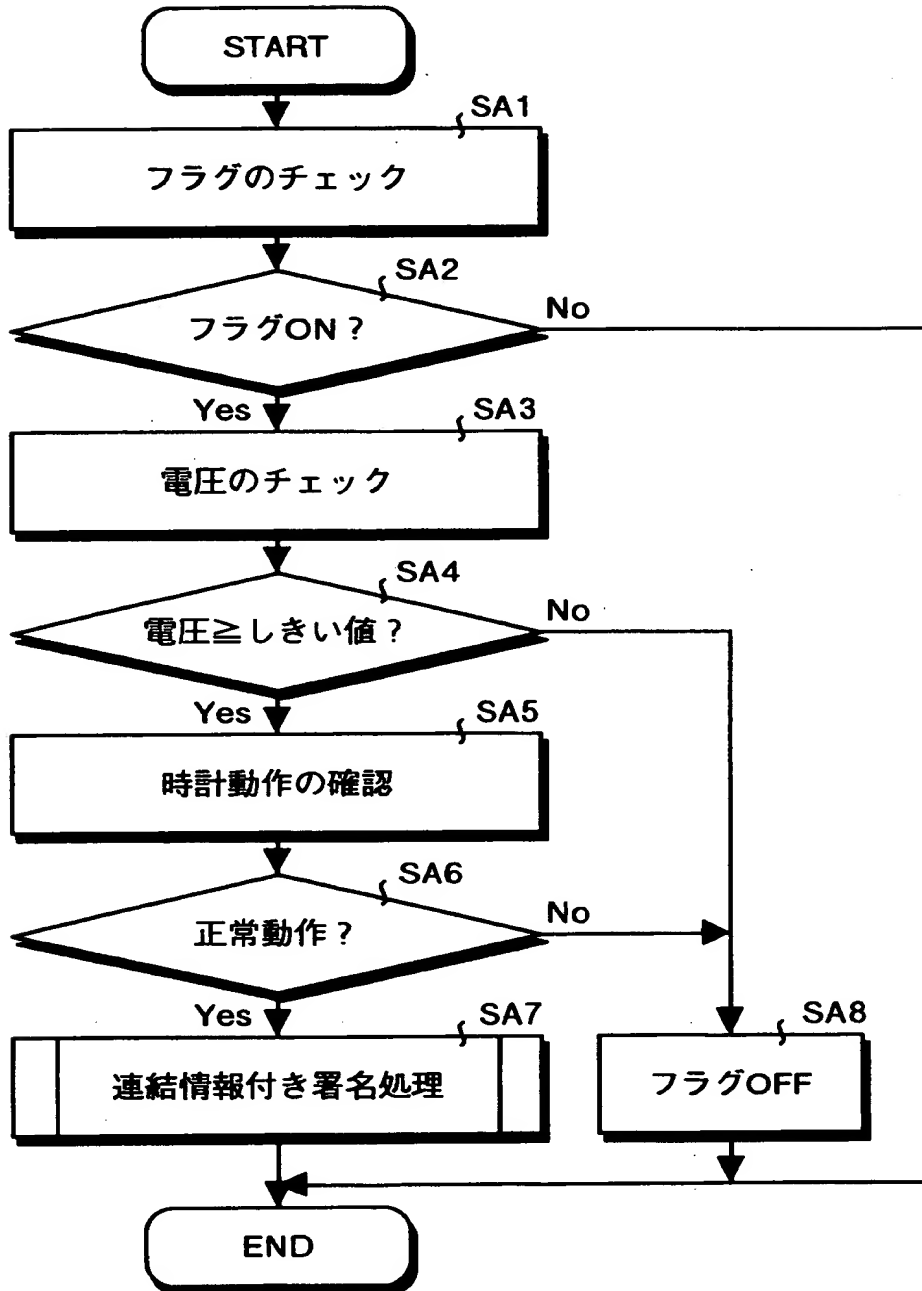
【図 4】

実施の形態 1 におけるデータ遷移を示す図



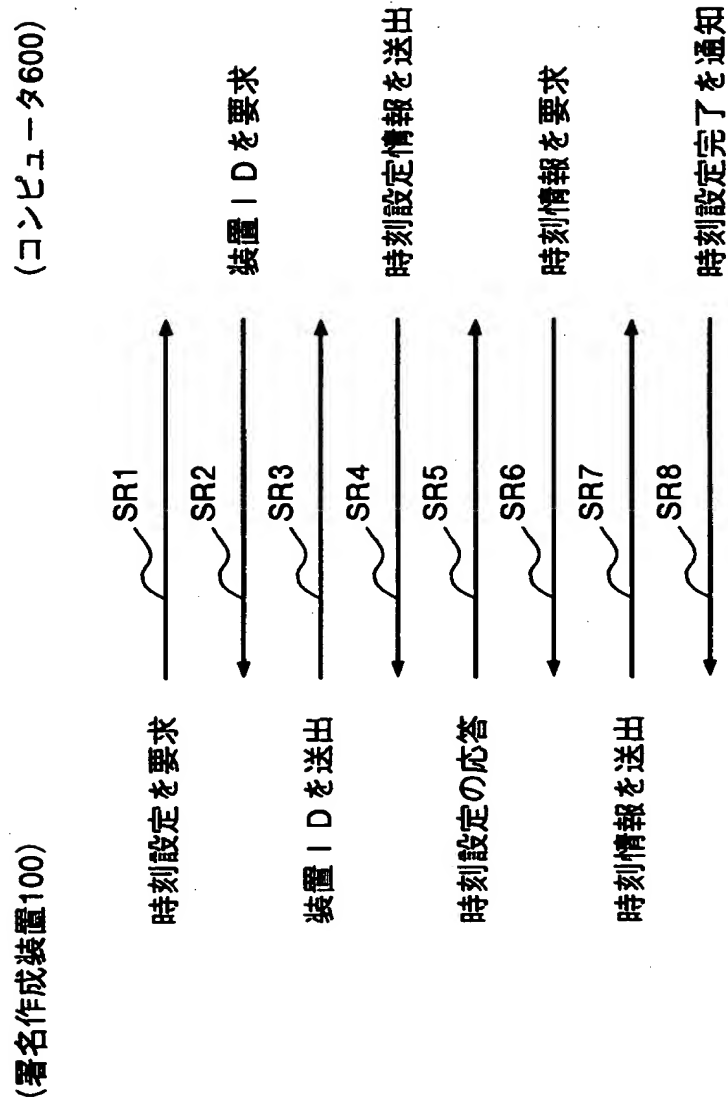
【図 5】

実施の形態 1 の動作を説明するフローチャート



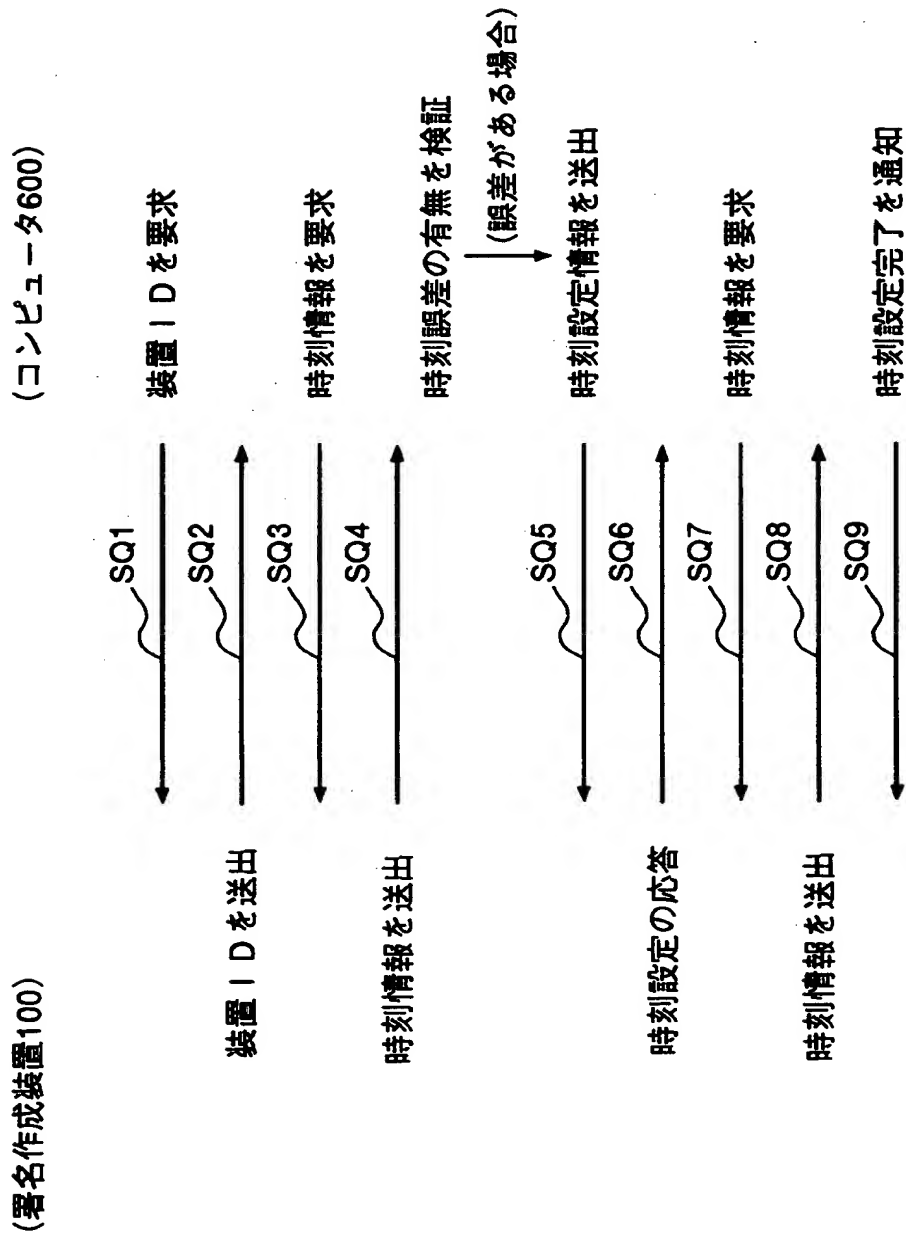
【図 6】

実施の形態 1 における時刻設定のシーケンスを示す図



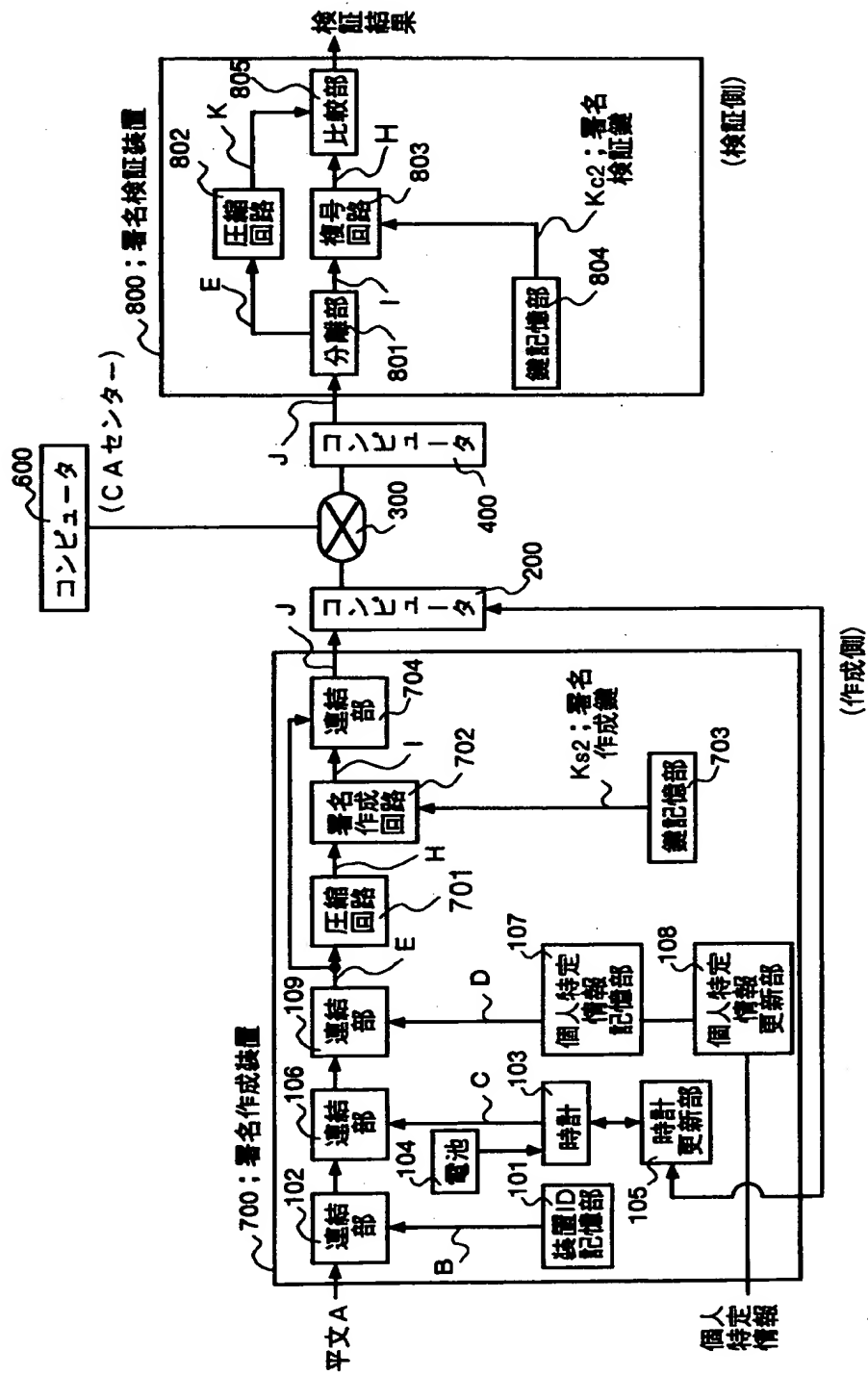
【図 7】

実施の形態 1 における時刻設定シーケンスを示す図



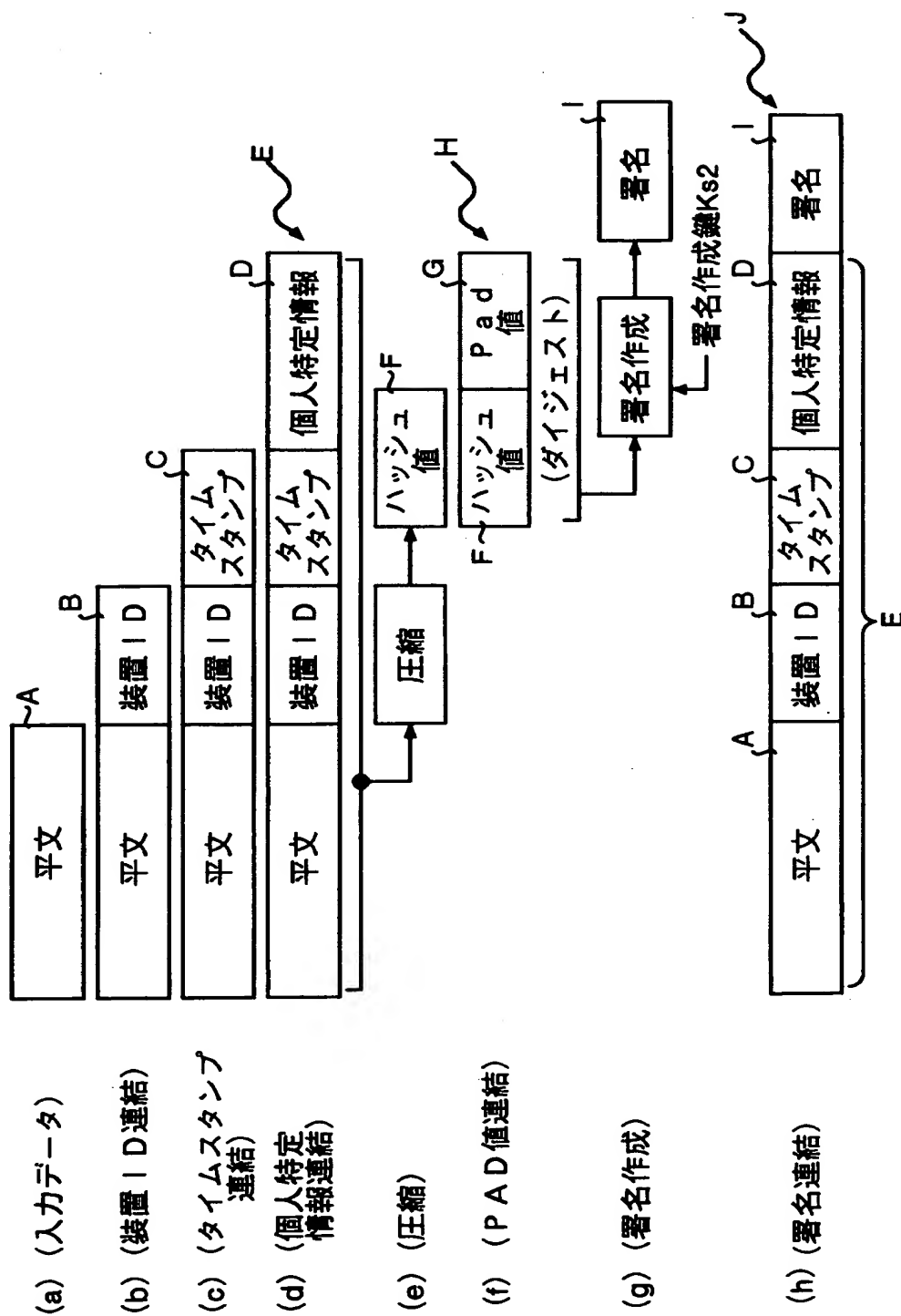
【図 8】

実施の形態 2 の構成を示すブロック図



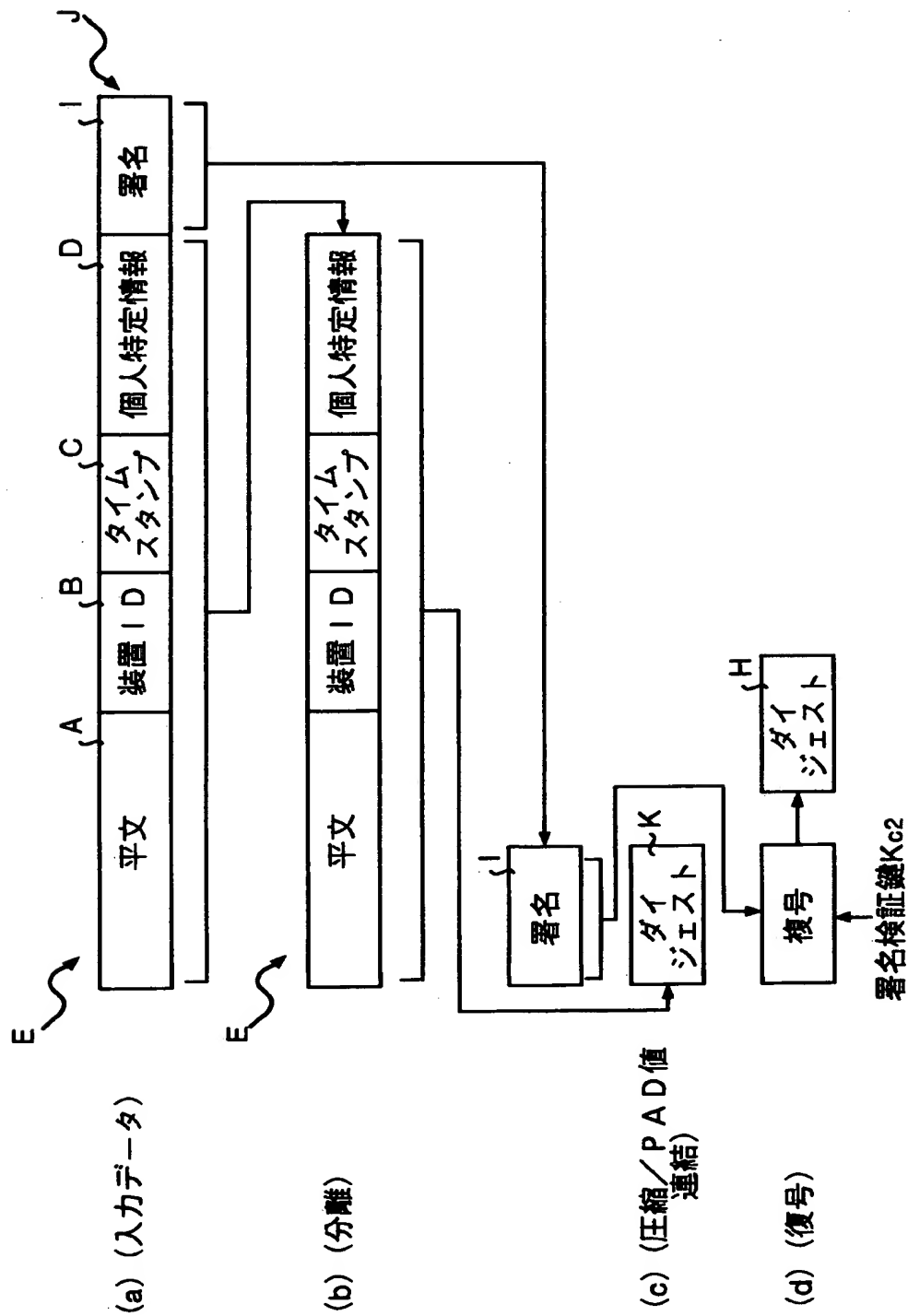
【図 9】

実施の形態 2 におけるデータ遷移を示す図



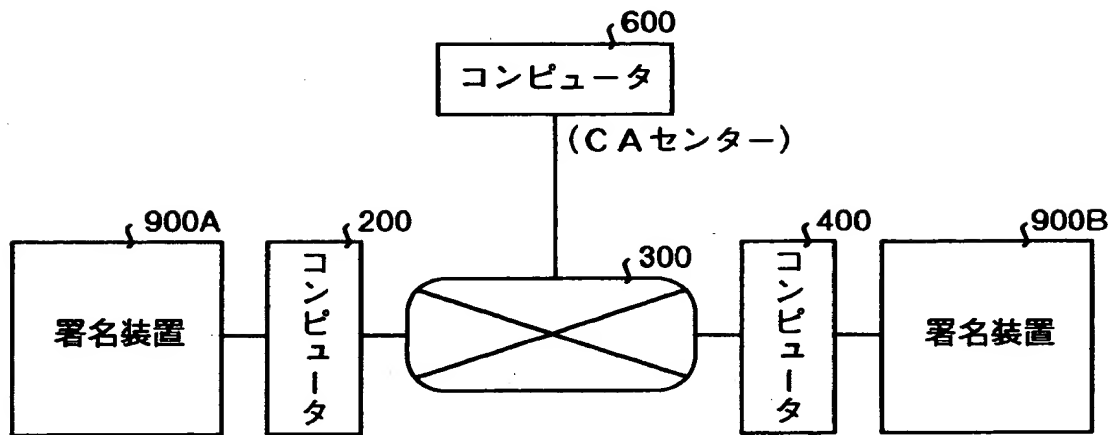
【図 10】

実施の形態 2 におけるデータ遷移を示す図



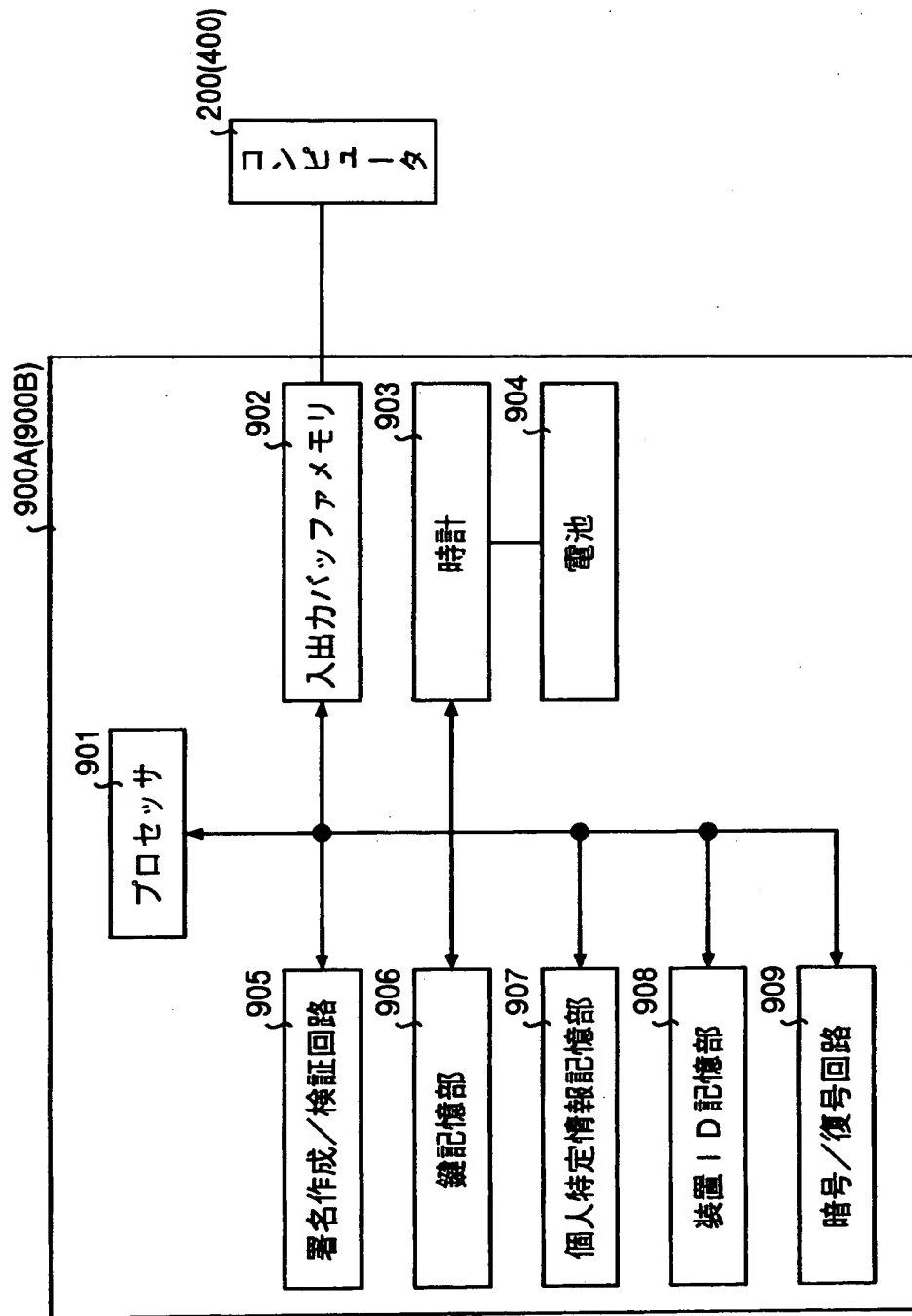
【図 11】

実施の形態 3 の構成を示すブロック図



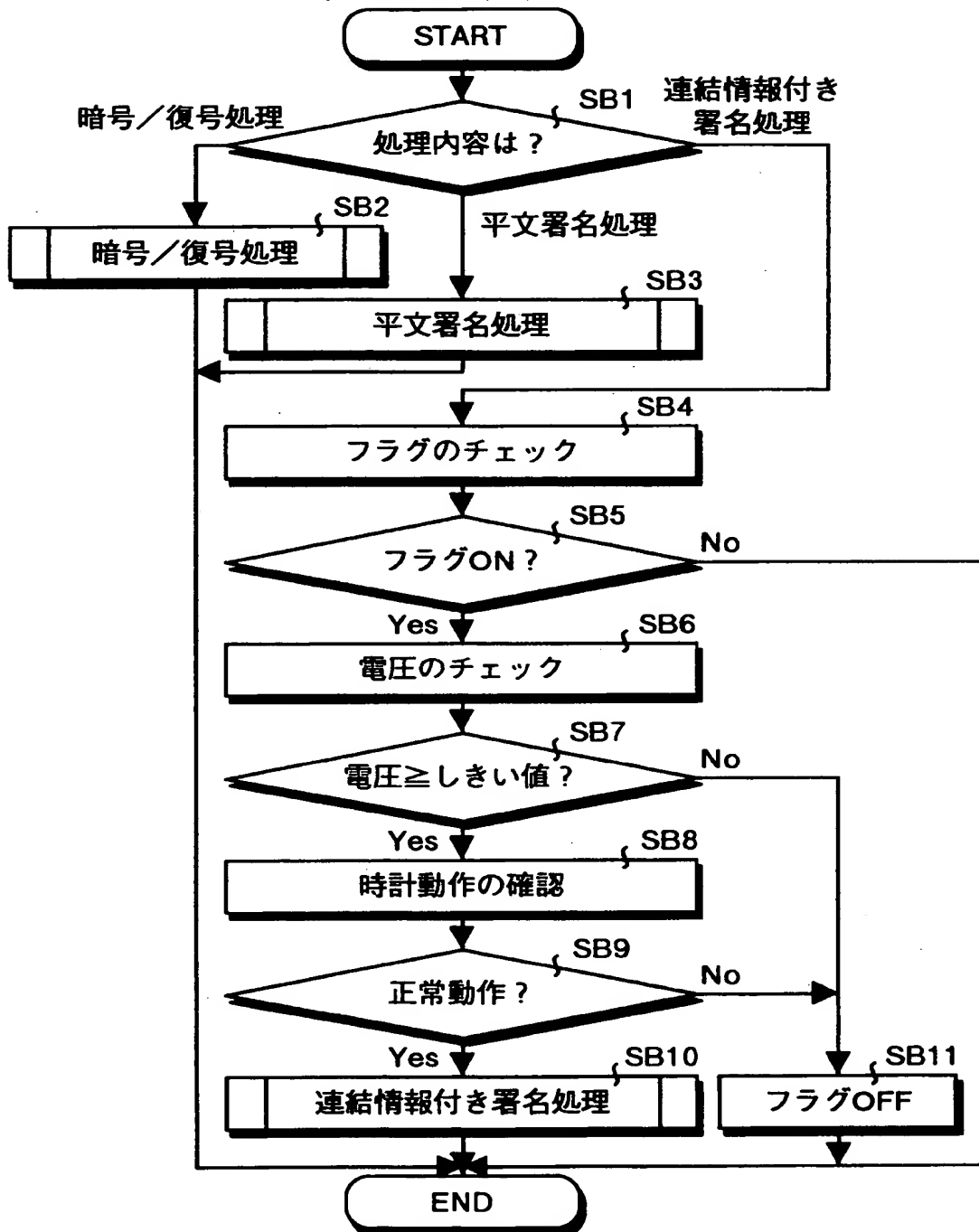
【図 12】

図11に示した署名装置900A (900B) の構成を示すブロック図



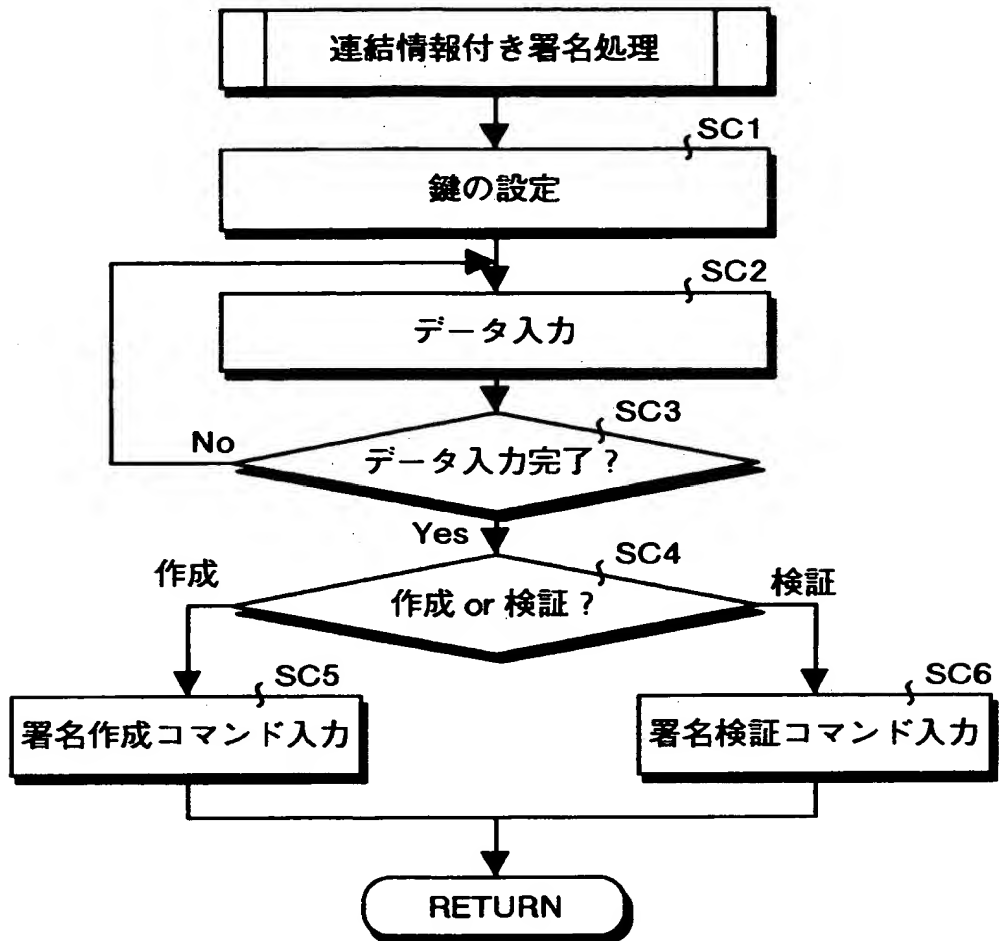
【図 13】

実施の形態 3 の動作を説明するフローチャート



【図 14】

実施の形態 3 における連結情報付き署名処理
を説明するフローチャート



【書類名】 要約書

【要約】

【課題】 日時の改竄を防止することができるとともに、デジタル署名を行った者、装置を特定することができ、しかも作成者に関する情報の変更柔軟に対応できる署名作成装置および署名検証装置ならびに署名装置を提供すること。

【解決手段】 デジタル署名の作成の日時の認証に用いられる日付、時刻等の時間に関するタイムスタンプCを生成し、CAセンターに設置されたコンピュータ600以外により時刻設定ができないようになっている時計103と、装置を特定するための装置ID・B、タイムスタンプCおよび作成者を特定するための個人特定情報Dを平文Aに連結することで署名対象データEを作成する連結部102、106および109と、署名対象データEを署名作成鍵 K_{c1} 等で暗号化し、署名Lを作成する署名作成回路112と、署名対象データEに署名Lを連結し、署名済みデータMとして送出する連結部113とを備える。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号

氏 名 富士通株式会社